TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

2€
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

HACKER JOURNAL

n. 167
www.hackerjournal.it

GAMES ON LINE
CRACCA & VINCI



HARDWARE
GADGET SICURI AL 100%

MOBILE
HACKERATI 4 GPS

WINDOWS VISTA
CREA LA TUA HACKER VERSION

P4P IL FILE SHARING SI EVOLVE

QUATTORD. ANNO 9 - N° 167 - 1/14 GENNAIO 2009 - € 2,00
WLF PUBLISHING

Anno 9 – N.167
1/14 gennaio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Internet e politica

"Non è forte colui che non cade mai ma colui che cadendo si rialza".
Johann Wolfgang von Goethe

Lo so, non è bello dire "l'avevo detto".

Sono passati pochi numeri, per la precisione dal 163 di Hacker Journal, da quando, osservando la reazione del Presidente francese Nicolas Sarkozy di fronte alla violazione del proprio conto corrente bancario, commentavo amaramente la differenza del suo comportamento con quello di gran parte dei politici italiani così distanti dal mondo legato a Internet e ai suoi linguaggi di comunicazione.

Recentemente Vittorio Zucconi, durante un'intervista radiofonica, ricordava come l'entourage di Barack Obama avesse saputo sfruttare al meglio la potenza di Internet per raggiungere tutti i propri sostenitori. Saper sfruttare significa conoscere.

Passa qualche giorno ed ecco che il raffronto con i nostri politici appare in tutto il suo grigiore. Un deputato del parlamento italiano nonché consigliere comunale, il colore e l'appartenenza politica non hanno nessuna importanza, non riuscendo più ad accedere al proprio account su Facebook non ha trovato nulla di meglio che presentare una "interpellanza parlamentare al ministero delle telecomunicazioni".
Ripeto una "interpellanza parlamentare".
Ripeto una "interpellanza parlamentare".
Ripeto una "interpellanza parlamentare".
E non smetterei di ripeterlo perché è davvero incredibile.

Con, ovviamente, il rituale adombrare di fantomatici "controlli dall'alto", "censure" e via dicendo.

In risposta molti hanno colto lo stridore di un'iniziativa del genere in un momento di grave crisi economica come quella attuale ma il punto non è questo. Il mio, e sono certo nostro, sbigottimento sarebbe stato assolutamente identico anche se ci fossimo trovati in una sorta di età dell'oro.

E, si badi bene , non voglio qui difendere Facebook perché a chiunque di noi darebbe fastidio, molto fastidio, non riuscire dall'oggi col domani e senza alcuna motivazione plausibile a raggiungere la propria rete di contatti; e molti di noi nella stessa situazione avrebbero fatto fuoco e fiamme, invaso di post i blog e dato vita a proteste assortite. Ma la politica è un'altra cosa.

Portare in parlamento una questione come questa significa non conoscere Internet. "Siamo abituati a politici che di Internet sanno poco o nulla".

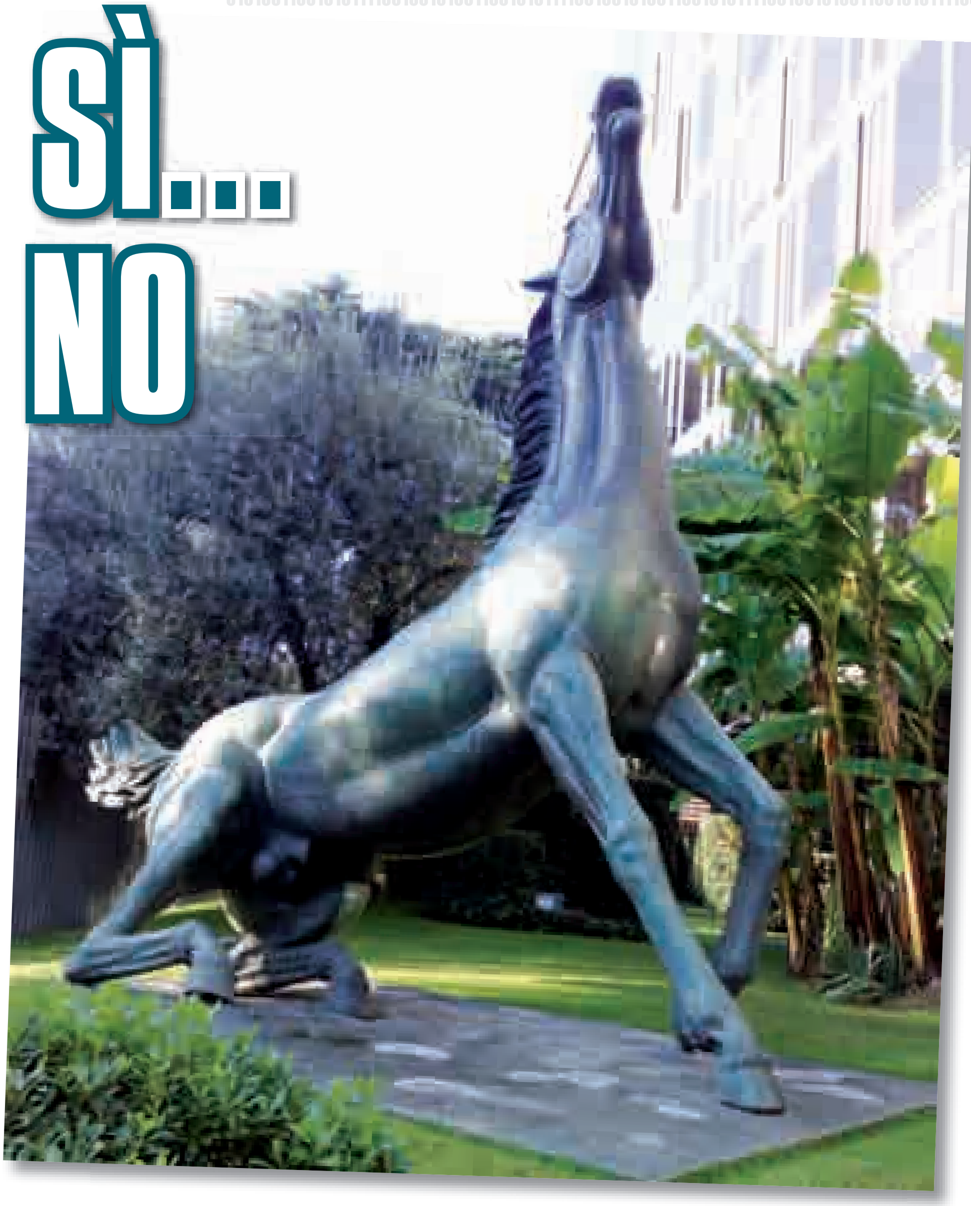
L'avevo detto

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE
Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Canone Sì... canone NO



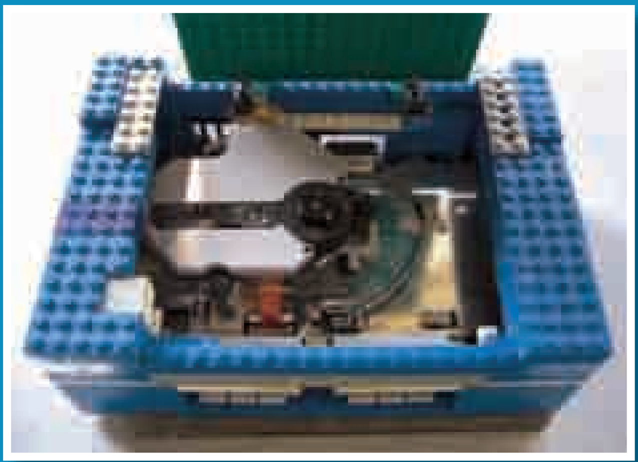
Abbiamo fatto un giro sul nuovo sito presentato dalla RAI che dovrebbe contenere tutte le informazioni utili per il cittadino a proposito del famigerato canone. L'unica cosa che risulta chiara è che bisogna pagare: non solo chi ha un televisore in casa e lo usa per guardare i reality show, ma anche chi dispone di un computer, un videocitofono, un lettore MP4, un iPod, un cellulare e chi più ne ha, più ne metta. Questo perché tutti questi apparecchi possono essere adattati alla ricezione di trasmissioni radiotelevisive. Perché in realtà noi non paghiamo il "canone RAI", ma "l'imposta sul possesso di apparecchi adatti o adattabili alla ricezione delle radioaudizioni", anche se non li usiamo e anche se non sono in realtà predisposti per guardare la TV o ascoltare la radio (chi è che lo fa sul videocitofono? Vogliamo conoscerlo!), dicitura talmente vaga che per assurdo potrebbero farci rientrare anche il nostro forno a microonde se ha un display un po' più complesso dei soliti numerini a LED a 7 segmenti...
Ma ciò che sta facendo scalpore è la differenziazione tra abbonamento ordinario, cioè quello che deve pagare la nostra famiglia, e abbonamento speciale, quello pagato da un'azienda che detiene un televisore o un apparecchio radiofonico: in quest'ultimo caso infatti risulterebbe escluso il PC, al contrario di quello ordinario che lo comprende (a dispetto di tutte le battaglie portate avanti anche dai vari governi per portare il PC stesso in tutte le case: una maniera per irretire nuovi abbonati?).
Da anni le associazioni dei consumatori si battono per l'abolizione del balzello, reputato ingiusto e sostanzialmente inutile, soprattutto da quando è la pubblicità la fonte di guadagno principale delle emittenti radiofoniche e televisive. Esistono anche sistemi per evitare del tutto di pagare il canone, che consistono nel "suggellare" i dispositivi (addirittura dovrebbero essere rinchiusi in un sacco di iuta piombato dall'ufficiale di Polizia Giudiziaria) in modo che non possano essere più usati.
Bene, a dispetto di tutte le battaglie portate avanti da ADUC, l'associazione dei consumatori che da anni si occupa direttamente della faccenda con petizioni e aiuti a chi non riesce a districarsi tra le norme che regolano il canone, siamo arrivati al punto in cui non solo la RAI pretende che si paghi il canone anche per gli oggetti più insulsi, ma addirittura chiede a gran voce un aumento.

DOWNGRADE RINCARATO

Da giugno scorso Microsoft non vende più Windows XP. Ma sono ancora molti gli utenti che, piuttosto di passare definitivamente a Vista, preferiscono aderire all'opzione di downgrade per tornare anche con il nuovo PC a Windows XP, soprattutto per quanto riguarda i notebook, più in difficoltà con Vista. Il problema però è che nel corso di soli sei mesi il prezzo richiesto per questa operazione dai produttori e rivenditori di computer è praticamente triplicato: Dell per esempio è passata dai 50 ai 150 dollari. Pare proprio un comportamento per disincentivare il downgrade e convincere più utenti possibile a rimanere con Vista. Fintanto che, naturalmente, non arriverà sugli scaffali Windows 7, che dovrebbe essere più adeguato per il funzionamento sui notebook.

TEMPO DA PERDERE

Mettiamo il caso di avere molto tempo libero e di non sapere come occuparlo. Mettiamo anche il caso di avere qualche conoscenza di elettronica, una vecchia Playstation lì sullo scaffale a prendere polvere e il classico bidone pieno di mattoncini Lego che non usiamo più dai tempi dell'infanzia. Bene, possiamo unire le tre cose e ottenere una bellissima PlayLego, una Playstation con il case completamente in mattoncini Lego. È quello che ha fatto uno studente un po' nerd e ha ottenuto l'esemplare unico che vediamo in foto, che naturalmente è perfettamente funzionante. Viene però da pensare: non sarebbe meglio uscire e correre dietro alle ragazze piuttosto che perdere tempo con videogames e costruzioni?



PIÙ WIMAX IN TOSCANA

Sta partendo in Toscana un'iniziativa di FreeMax S.p.A. per la fornitura di servizi di connettività wireless per tutti, dal privato all'azienda, con varie modalità di abbonamento flat a prezzi molto convenienti. Secondo Eric Le Bihan, patron di FreeMax, la Toscana è una regione un poco dimenticata per quello che riguarda la connettività. Dato che la sede aziendale si trova proprio in Toscana, l'azienda ha una buona conoscenza della realtà locale e si sente quindi in grado di sopperire alle mancanze di altri operatori. Nasce così l'accordo con Retelit S.p.A. che fornirà l'infrastruttura e le frequenze, mentre FreeMax si occuperà della raccolta abbonamenti e della distribuzione dei dispositivi di connessione. Le offerte partono da 19,89 euro al mese per la navigazione wireless in tutta la propria città a una velocità intorno ai 4 Mbps (2 Mbps garantiti).





I CELLULARI SI RICARICANO DA SOLI



È uno studio portato avanti da Intel: lo scopo è quello di raccogliere il più possibile le cosiddette "energie libere", cioè calore, movimento e onde elettromagnetiche, e usarle opportunamente convertite per ricaricare le batterie di dispositivi portatili come lettori MP3 e cellulari. L'obiettivo finale è il dispositivo privo di batteria che non ha bisogno di ricarica: unendo tutte le tecnologie disponibili e tutte le fonti energetiche contemporaneamente, il dispositivo ideale non avrà bisogno di essere collegato a un caricabatterie e chi lo usa potrà tranquillamente "dimenticarselo" acceso, certo che, al momento del bisogno, sarà presente carica sufficiente per compiere l'azione desiderata. Una manna per chi continua imperterrito a dimenticare a casa il caricabatterie del telefonino.

FALLITO IL P2P COMMERCIALE

BitTorrent Entertainment Network doveva essere l'esperimento P2P in mano alle majors dell'intrattenimento per dirottare il traffico illegale delle reti P2P tradizionali sul proprio canale controllato e, naturalmente, a pagamento. Il risultato è stato praticamente un fiasco completo. Già da tempo in corso di ristrutturazioni aziendali e tagli di personale, l'azienda è stata costretta dall'indifferenza generale del popolo del peer to peer a rivedere i propri obiettivi commerciali. È nella natura delle cose, questo almeno dovevano prevederlo: non si può pretendere di imbrigliare nelle maglie commerciali e controllate qualcosa che nasce liberamente e spontaneamente, ne è prova il fatto che in Rete si trova sempre e comunque di tutto per quanto qualcuno cerchi di controllarla.

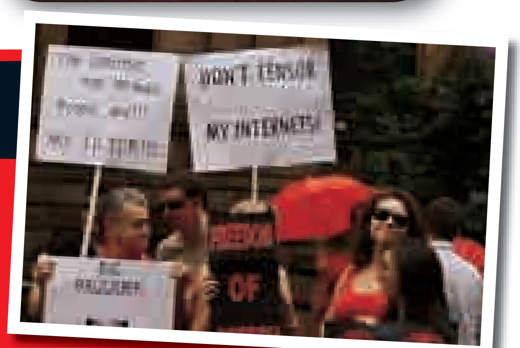
BitTorrent

CIAO CIAO TASTIERA

Secondo il Pew, centro di ricerca americano che si occupa prevalentemente di previsioni sul futuro, ne è praticamente certo: nel 2012 il modo di controllare i computer sarà cambiato radicalmente, grazie alle nuove tecnologie. I visionari ricercatori ipotizzano un'interfaccia priva di tastiera e mouse, comandata prevalentemente via voce o, se proprio non siamo dell'umore adatto per parlare col PC, attraverso una tastiera virtuale proiettata sulla superficie del piano di lavoro o su altro supporto. Dalle ricerche del Pew risulta anche un altro importante scenario: la scomparsa dei DRM, fondamentalmente inutili data la "bravura" dei pirati e senza ombra di dubbio un grande fastidio per gli utenti normali.



In strada contro i filtri



In Australia il popolo degli internettiani è sceso in piazza per protestare apertamente contro i filtri sui contenuti che il governo pare voglia implementare. Secondo i naviganti australiani non è Internet a essere bacata, ma le persone che la frequentano: guai a intaccare la libertà di ognuno di fruire dei contenuti che più gli aggradano, piuttosto prendetevela con chi pubblica e distribuisce materiale illegale o immorale, ma non "punite" tutti. Secondo il ministro delle Comunicazioni Stephen Conroy quei filtri serviranno a proteggere gli utenti da contenuti illegali e immorali, ma gli utenti stessi non sono d'accordo e temono invece un abuso di controllo da parte del governo stesso. Al coro dei protestanti si aggiungono anche le voci dei provider, che dovranno essere gli esecutori materiali delle decisioni che verranno prese dal governo.

USB 3.0 GIÀ SU LINUX

Sono già state pubblicate le specifiche della terza generazione dello standard USB, almeno per i produttori e gli sviluppatori. Contrariamente a quanto si possa pensare, però, non sarà Windows ad avere la precedenza nel rendere disponibile lo standard nel prossimo futuro: tutto fa presagire che il primo sistema operativo a supportare collegamenti USB ad altissima velocità sarà Linux, grazie anche all'aiuto ingente che la comunità del pinguino sta ricevendo da Intel.



La stessa Intel infatti sta sviluppando un driver open source che supporti le nuove specifiche da integrare nelle prossime release del kernel di Linux, che così per la prima volta sarà un passo avanti rispetto al sistema operativo di Microsoft. Non vediamo l'ora!

PLAYSTATION HOME BUCATA

È passato pochissimo tempo dal lancio dell'area social networking di Sony dedicata agli appassionati di Playstation 3, e già sono spuntati giudizi poco favorevoli da parte di hacker e smanettoni che hanno sondato il sistema alla ricerca di falle e problemi. Che, naturalmente, sono stati trovati e in gran quantità: StreetskaterFU ha pubblicato sul suo blog (http://streetskaterfu.blogspot.com/2008/12/home-release-special-home.html) un elenco dettagliato dei bachi e di cosa si può fare se solo si sa dove mettere le mani. Secondo l'hacker si tratta di codice vecchio e malformato, addirittura risalente a tecnologie del 2005, momento in cui presumibilmente è stata iniziata una lavorazione dilungata fino a oggi.





RECAPTCHA
RE DEI CAPTCHA

Abbiamo già visto (HJ 164) che i Captcha non hanno vita lunga: anche quelli più complessi che visualizzano lettere e numeri su sfondi confusi infatti sono stati prima o poi craccati, permettendo libero accesso agli spammer di ogni tipo. Addirittura, anche gli ultimi tentativi di produrre un Captcha complesso che usi immagini o audio non hanno dato buoni frutti. Tutti, tranne reCaptcha. Questo sistema usa parole digitalizzate da libri e da vecchi numeri del New York Times distorti sufficientemente per essere leggibili all'occhio umano ma non da un bot. Forte di questo successo, reCaptcha vuole tentare anche con Captcha audio per chi ha difficoltà di vista. Speriamo con gli stessi risultati.



ARRIVANO LE ZZZ MAIL

In realtà la versione che potremo È stato documentato il primo caso al mondo di e-mail sonnambule, inviate cioè inconsciamente durante il sonno. È successo a una donna di 44 anni che, profondamente addormentata, si è alzata, ha acceso il PC, attivato la connessione a Internet inserendo nome utente e password



HOT NEWS

URU LIVE È OPEN SOURCE

Per chi non lo conosce, Uru Live è il MMORPG basato su Myst che è stato punto di raccolta per molto tempo di tutti gli appassionati del gioco d'avventura. La crisi finanziaria sta colpendo anche le industrie video ludiche, e, a detta dei responsabili di Myst, se non avessero preso questa decisione probabilmente Uru Live sarebbe stato destinato al dimenticatoio, dato che non ci sono più i fondi per finanziare il progetto. Da qui la decisione: i codici di client, server e tool sono stati rilasciati in open source, per dare modo agli appassionati di tutto il mondo di aprire il proprio server e contribuire così ad allungare la vita al gioco. Un'iniziativa che ci fa piacere e che speriamo non rimanga isolata nel mondo dei videogiochi.

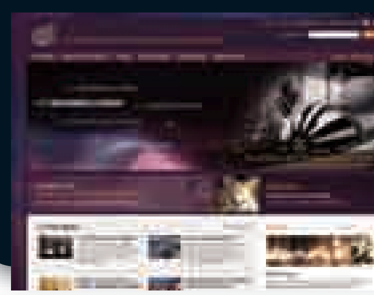


GROSSI GUAI PER INTERNET EXPLORER

Ancora una volta, si potrebbe dire, tanto siamo abituati ad annunci di questo tipo. Comunque, ecco la notizia: è stata scoperta una nuova grave falla di sicurezza per Internet Explorer. Questa falla inizialmente sembrava riguardare solamente gli utenti di XP e Internet Explorer 7, ma a quanto pare tutte le versioni di Internet Explorer a partire dalla 5.01 ne sono affette, compresa la nuova versione 8 ancora in fase di test. Ancora più grave è il fatto che non sia al momento prevista alcuna patch che risolva il problema e non si sa nemmeno se e quando verrà sviluppata. Microsoft dice che è possibile proteggersi impostando il livello di sicurezza sul Web ad Alto e disabilitando l'esecuzione di Ole32db.dll via access control list. Ma sappiamo noi come proteggerci veramente: cambiamo browser!

ASI RINNOVA IL SITO

È finalmente online il nuovo sito dell'ASI, l'Agenzia Spaziale Italiana. L'aspetto grafico è notevolmente migliorato, così come la navigabilità, e già da una prima occhiata appare ricco di contenuti e di informazioni, che nella precedente versione erano un po' disorganizzati e deludenti. Segno che anche in Italia, finalmente, si sta dando la dovuta importanza al settore aerospaziale: non che prima non ne avesse, ma ora ha il giusto peso anche l'opera di divulgazione e informazione. Anche chi non mastica l'inglese, quindi, avrà modo di tenersi aggiornato su cosa combinano tra le stelle i nostri astronauti, senza la necessità di andare a visitare il sito dell'European Space Agency o, peggio, quello della NASA. L'indirizzo per gli appassionati è www.asi.it.



e ha inviato tre e-mail ad altrettanti amici chiedendo loro di portare caviale e vino. Non è una burla, tant'è che ne ha parlato la rivista scientifica Sleep Medicine. I medici hanno riconosciuto l'originalità del caso e lo hanno classificato come il primo esempio di "zzz-mail". A parte gli scherzi, non è raro di sentire di persone che sono rimaste alzate fino a tardi davanti al computer e a Internet (tutti noi l'abbiamo fatto almeno qualche volta), incantati chattando o sfogliando Facebook e simili. Che sia l'inizio di un nuovo disturbo della salute tecnologico?

CHROME RIMPIAZZA FIREXE

A dispetto di tutto quello che è stato detto finora a proposito del browser di Google, alla troppa fretta con cui è stato pubblicato e ai vari problemi che lo affliggono, la casa di Mountain View ha deciso che la prossima release in inglese di Google Pack (il pacchetto di software gratuito proposto in bundle da Google stessa) conterrà il proprio browser invece di Firefox 3. A nostro avviso si tratta di una decisione un po' avventata, ma gli sviluppatori di Google credono tanto nel loro pupillo da anticipare di nuovo una promozione che forse il pubblico non è ancora pronto a recepire inserendolo nel pack, invece di aspettare e sviluppare nel frattempo le versioni per Linux e MacOS X. A dispetto dei 10 milioni di utenti vantati da Chrome.



Nuove forme di raggiro iniziano a farsi vedere su Internet

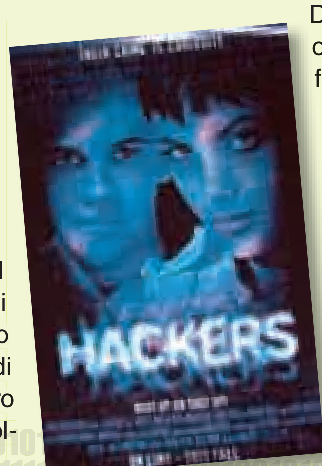
CHIAMAMI... e ti TRUFFO

Social engineering: ecco il termine con cui si definisce la tecnica di raccolta di informazioni sensibili a spese di persone poco accorte che, ingannati da un interlocutore scaltro che si finge plausibile, sono spinti a fornire credenziali, numeri di carte di credito e molto altro ancora.
In realtà nulla di nuovo: è una tecnica che ha fondamenti di psicologia che probabilmente è sempre esistita, ma che solo negli ultimi decenni ha trovato un nome e una precisa collocazione nell'ambito della ricerca sociale.

:: Visto al cinema

Dade è nella sua camera, smanettando un po' il suo nuovo computer. Alza il telefono e dall'altra parte risponde Norm, della sicurezza.
"Ciao Norm, sono Eddie Veder della contabilità, mi si è rovinato un file su cui stavo lavorando e ho bisogno di prelevarne una copia da lì, non è che mi dici il numero scritto sull'etichetta del modem? Quella scatoletta vicino al computer?" – "OK, 212-555-4240".

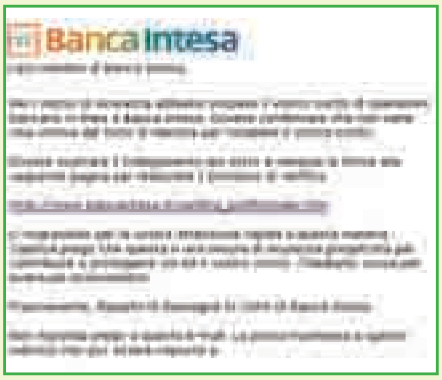
L'abbiamo visto al cinema nel film Hackers, uno dei primi della mitica Angelina Jolie. Non si tratta solo di finzione cinematografica, è una vera e propria tecnica di social engineering: fingersi qualcuno di accreditato per indurre il facilone di turno a darti quel numero di accesso, così puoi collegarti con il tuo modem alla rete interna dell'azienda e fare un po' quello che ti va, come cambiare programma televisivo o scatenare una guerra termonucleare globale simulata.



Da questa tecnica hanno avuto origine tutte quelle moderne, fino ad arrivare al phishing.

:: Gettiamo la rete

Phishing è di per sé una storpiatura della parola inglese fishing, l'azione di pescare. Con il phishing si getta una rete, costituita da un'e-mail fasulla ma plausibile contenente il collegamento verso un sito costruito ad hoc,



Un'e-mail contenente un tentativo di phishing. Siamo agli albori, notiamo l'italiano davvero ridicolo!

e si aspetta che la gente ci caschi, come bei pescioni, facendo clic sul collegamento e compilando diligentemente il modulo con i loro dati sensibili: login e password per l'accesso al conto bancario, numero della carta di credito, dettagliati dati personali per rubarne l'identità e così via. Queste e-mail fasulle hanno circolato parecchio anche in Italia, ma sono state quasi tutte inviate dall'estero, principalmente dall'est (Russia e Cina in testa). Il problema per questi malfattori è la lingua: l'italiano non è facile nemmeno per noi italiani, figuriamoci per un russo o un cinese che usa un traduttore automatico. Il risultato è che le mail inviate come esca nelle nostre caselle di posta erano completamente improponibili e improbabili, qualcosa per cui valeva la pena farsi due risate (diciamocelo, "scattate la bandiera" invece di "fate clic sul banner" fa veramente ridere) e passare oltre. Se vogliamo passare qualche minuto di piena ilarità, ci basta visitare qualche sito che pubblica il testo delle e-mail di phishing, come http://truffeinrete.wordpress.com/2008/11/17/gentile-signor-bancoposta/ (Gentile Sig. Bancoposta?!?) oppure http://zadoo.wordpress.com/2008/10/30/bpm-avviso-importante-no-1225193196/ (Caro membro di Gruppo BPM??).

:: Piccoli pescatori crescono

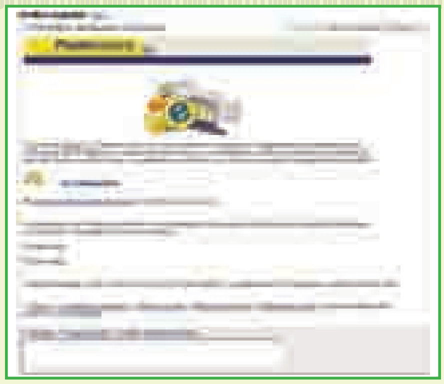
Ma il criminale informatico di oggi è principalmente un imprenditore, che investe anche per migliorare il proprio "servizio". Ecco quindi che, di punto in bianco, le e-mail di phishing sono diventate plausibili: siti istituzionali di banche e poste riprodotti a dovere, la cui falsità è riconoscibile solamente analizzando minuziosamente l'indirizzo della pagina o del collegamento contenuto nel testo, e anche l'italiano proposto è degno di fiducia, perché il messaggio è stato tradotto da una persona che l'italiano lo sa.
Ma ormai, si spera, siamo tutti abbastanza smaliziati da riconoscere ugualmente una di queste e-mail, e da contattare l'ente da cui pare provenire per avere una conferma prima di intraprendere qualunque tipo di azione a partire dal clic sul collegamento.

:: Se non clicchi, chiama

Oggi inizia a diffondersi una nuova tecnica di ingegneria sociale volta alla raccolta di informazioni, che gli esperti hanno subito battezzato "vishing". La truffa avviene via voce: la solita e-mail fasulla non invita più a fare clic su un collegamento, ma a chiamare un numero VoIP. Oppure, analogamente, il computer del malfattore chiama sequenzialmente dei numeri di telefono, aspettando che qualcuno risponda. In entrambi i casi, un messaggio registrato nella lingua del destinatario invita a chiamare un numero (sempre VoIP) fatto passare per quello del servizio antifrodi della banca, delle poste eccetera.



Non bastano più banche e poste: ora anche McDonald's e Coca Cola vengono imitate dai phishers. Naturalmente l'allegato è un trojan.



Questa invece è una delle e-mail più recenti. La lingua e l'aspetto sono notevolmente migliorati, tanto che iniziano a essere pericolose.

A quel punto scatta la tecnica di social engineering vista in Hackers: risponde il malfattore in persona, oppure una persona compiacente che sappia la lingua della vittima, e inizia la raccolta dei dati personali, dei numeri di carte di credito e così via.
Ma davvero è così facile cascare in questo tranello? Non ci fa insospettire un po' che un impiegato della nostra banca ci telefoni a un orario improponibile per chiederci i nostri dati parlando con accento straniero?

E poi, diciamocelo chiaro: se stiamo attenti al momento dell'accettazione delle condizioni di qualunque contratto di fornitura di servizi online, è praticamente sempre riportato il fatto che nessuno dei dipendenti della banca in qualunque posizione lavori è autorizzato a chiedere nome utente, password o altri dati che riguardano il nostro accesso al servizio, quindi se ci pareva convincente la conversazione fino a quel punto, nel momento stesso in cui chiedono questi dati sappiamo per certo che non si tratta in realtà di un impiegato della banca. Inoltre, ancora a monte, perché dovremmo telefonare a numeri strani e particolari invece che a un numero verde che di solito conosciamo a memoria?
Non ci resta che attendere di fare quattro risate sentendoci dire da una voce improponibile "Puonciorno Sighnor Pancoposta".

Da Verizon arriva una nuova tecnologia che permette trasferimenti più veloci

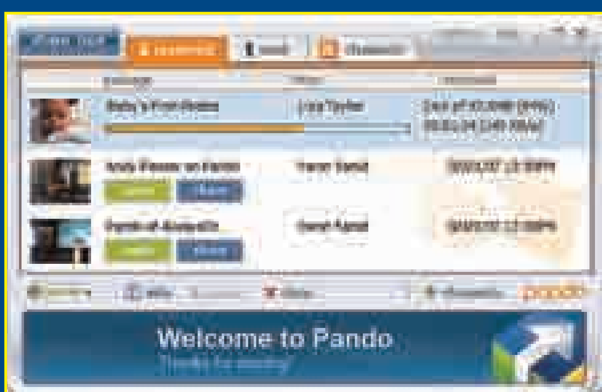
P4P: EVOLUZIONE DI UNA SPECIE

Quando troviamo un file interessante nelle reti peer to peer sappiamo già che prima di poter aprire il file, il più delle volte, per la fine del download potrebbero volerci ore come giorni, dipende dalla disponibilità del file, dalla velocità della rete e dalla fortuna.

Da oggi però le cose potrebbero cambiare. Grazie a una nuova tecnologia denominata P4P, studiata e implementata da Verizon insieme a Pando Networks e chiamata per l'appunto Pando.

:: Lo stato attuale

Rinfreschiamoci un po' la memoria: il peer to peer non è certo una tecnologia nuova, ormai sono oltre 10 anni che esistono diverse implementazioni del concetto di base. Per definire delle pietre miliari, possiamo iniziare da Napster, il primo grande motore di ricerca e scambio di musica online, passando per le varie reti Gnutella, DC++ e eDonkey, che hanno segnato il boom del peer to peer in ogni ambito, per arrivare alla tecnologia Torrent. Il funzionamento di tutte queste reti è piuttosto simile: i server centrali raccolgono elenchi di peer (i singoli utenti) e dei file da questi condivisi; il peer interessato a un file quindi viene messo in diretto contatto con uno o più utenti che lo condividono e, in base al funzionamento del programma, ha inizio il trasferimento da una singola fonte oppure da più fonti. In sostanza, il server mette solo in comunicazione i peer e non conserva i file in locale: i file stanno solo sui computer degli utenti e vengono trasferiti direttamente a chi ne fa richiesta.



Una schermata di Pando, il software di Pando Networks che implementa una nuova maniera di fare peer to peer.

:: I problemi di oggi

Innanzitutto bisogna dire che i problemi sul trasferimento sono soggettivi: non si tratta quindi di problemi dovuti alla tecnologia, ma al comportamento degli utenti. Più un file viene mantenuto in condivisione da chi l'ha già sca-

ricato, più sarà facile per altri utenti trovarlo e scaricarlo. Inoltre, dato che quasi tutti i programmi permettono di impostare la banda a disposizione dei trasferimenti peer to peer, non è detto che tutti lascino abbastanza banda per un upload decente: se, per esempio, un file è condiviso da poche persone e queste lasciano 10K di banda in upload con il minimo di connessioni, ognuna di esse potrà servire al massimo due o tre utenti, che scaricheranno a circa 3K al secondo. Pur scaricando da più fonti, ed è molto raro, ci vuole comunque un tempo abbastanza lungo per terminare un download che a piena banda sarebbe durato al massimo qualche ora.

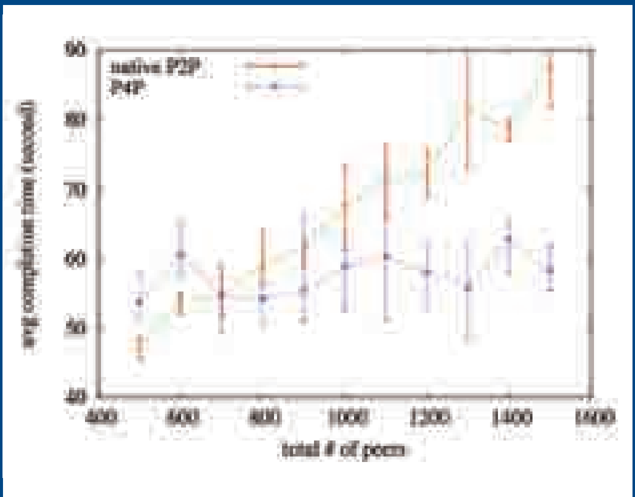
C'è un altro fattore da prendere in considerazione. Dato che la maggior parte del traffico peer to peer è costituito da file per lo più illegali (film, software e musica, tutto materiale coperto da diritti d'autore), è in corso una vera e propria guerra tra le industrie dell'intrattenimento e del software e gli utenti.
Al punto che vengono tirati in ballo gli stessi provider: oggi sono pochi quelli che non filtrano il traffico sulle porte comunemente usate dai software come eMule e simili, limitando pesantemente la banda.



Lo schema della rete Pando così come viene pubblicata sul sito. Da notare la presenza dei normali peer e del server centrale che fa anch'esso da fonte.

:: Come funziona il P4P

L'idea di Verizone e Pando risolve alcuni di questi problemi e promette, secondo gli studi effettuati, un incremento della velocità di trasferimento di un terzo, abbassando nel contempo del 60% la banda sprecata dai provider. Questo obiettivo viene raggiunto sommando gli effetti di due nuovi concetti che vanno ad affinare e migliorare la tecnologia peer to peer attuale.



Il grafico dell'incremento di prestazioni promesso da Pando.

Per prima cosa, viene sfruttata l'informazione geografica offerta dagli indirizzi IP. Secondo gli ingegneri Verizon (ma è un concetto limpido, che non fa una grinza) è inutile e dispendioso scaricare porzioni di un file "a caso", prendendone una parte in Italia, una in Germania, una in USA e una a Taiwan. Queste ultime due frazioni impiegheranno un tempo sensibilmente maggiore a giungere a destinazione e occuperanno banda su tutta la connessione tra noi e il provider sito in Taiwan. Se il software desse priorità ai peer geograficamente più vicini a noi, ci sarebbe un bel risparmio per tutti: per i provider lontani che non verrebbero interessati dal trasferimento, e per noi in termini di tempo di attesa. La tecnologia Pando quindi studia la topografia della rete di collegamenti per individuare il medesimo file dai peer più vicini a noi.

Un secondo aspetto, che farà storcere il naso a molti riguarda il fatto che tra i file disponibili non troveremo certo il film uscito al cinema la settimana scorsa, o l'ultima versione di Windows hackerata. I contenuti offerti da Pando sono esclusivamente legali, ovvero contenuti per cui l'autore ha espressamente scelto il P4P come mezzo di diffusione dell'opera. Se da una parte questo può sembrare limitante, dall'altra ha il suo vantaggio nell'aspetto velocità in quanto permette di costituire server centralizzati che ospitino non solo elenchi di peer ma i contenuti stessi, fungendo anch'essi da fonte per il trasferimento. Ma vediamo in dettaglio come funziona.

:: La rete Pando

La differenza tra una rete peer to peer classica e una rete Pando è la presenza di un filtro interno al provider che non serve per limitare la banda, ma per verificare da dove provengono le varie connessioni. In questo modo è possibile stabilire delle priorità tra le varie fonti disponibili: la precedenza va a quelle interne al provider, per non sprecare banda da e verso l'esterno inutilmente. Inoltre, il server Pando conserva una copia del file in trasferimento perché rimanga disponibile per più tempo possibile.
In questo modo chi scarica avrà a disposizione una fonte certa e veloce, il server Pando, e una o più fonti variabili che sfruttano la connessione P2P classica ma con precedenza geografica. Semplice e geniale.

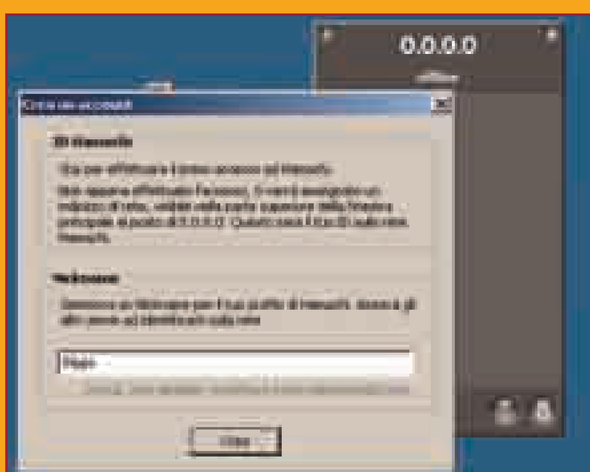
Connettiamo due computer a distanza con una VPN che permette anche di chattare

Incontri ravvicinati del... primo tipo

Tutto è nato dall'esigenza di scambiare velocemente e senza tante complicazioni dei dati con il mio amico Zot. In un primo momento abbiamo cercato di non usare nulla e di sfruttare ciò che Windows mette a disposizione, sia volontariamente sia involontariamente (sfruttando i noti problemi di sicurezza delle condivisioni). Ma su sistemi che vengono aggiornati continuamente questo approccio non conviene. Inoltre lui ha un PC dietro un firewall e io ho una struttura di rete un po' complessa con firewall e proxy. Pensa e ripensa alla fine abbiamo optato per Hamachi, un programma dal nome un po' buffo ma che alla fine si è dimostrato un software valido e robusto, facile da configurare e da gestire. Questo crea una scheda di rete virtuale sul nostro PC, con un proprio indirizzo IP, che può essere usata per collegarsi a reti Hamachi già esistenti (per esempio create da nostri amici) oppure per crearne una nostra e permettere ai nostri amici di accedere alle nostre condivisioni.

:: Installazione

L'installazione è molto semplice, basta scaricare il file da www.hamachi.it, eseguirlo e seguire le istruzioni che ci fornisce il sistema; l'unica raccomandazione è quella di utilizzare nomi di computer leggibili e password complesse. Soprattutto a quest'ultime dobbiamo dedicare un occhio di riguardo. Infatti, una volta "indovinata" da un malintenzionato, questo si garantirebbe il completo accesso al nostro sistema. Il setup di Hamachi ci chiede se installare il programma come servizio di Windows o se avviarlo normalmente. È buona regola avere sempre il pieno controllo di tutte le applicazioni quindi scegliamo la seconda opzione. Viene poi mostrata una finestra in cui l'installazione ci chiede se disabilitare i servizi di rete per Hamachi per motivi di sicurezza. Visto però che lo stiamo installando proprio per poter usare quei servizi, li teniamo abilitati senza spuntare la casella. Infine ci verrà chiesto se vogliamo usare la versione commerciale in prova o quella gratuita. Scegliamo pure quella gratuita, più che sufficiente per il nostro scopo



La scelta del nostro nickname sulla rete Hamachi.

:: La configurazione

Una volta installato tutto al primo avvio del programma ci vengono chieste alcune informazioni relative alla creazione del nickname con cui gli altri utenti ci vedranno e ci raggiungeranno via rete. Hamachi tenterà a questo punto una connessione basandosi sui dati utilizzati da Internet Explorer,

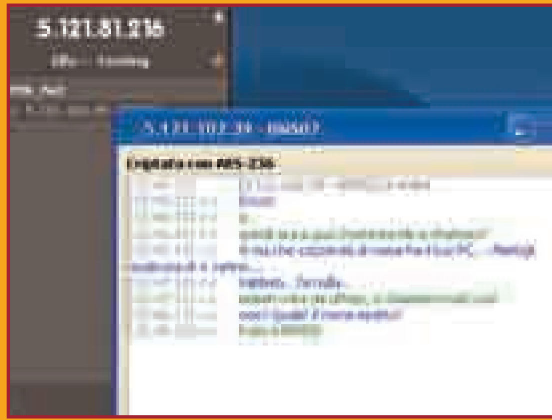
ma non sempre riesce a leggerli correttamente e può quindi capitare di ricevere una notifica di errore. Per raggiungere i menu di configurazione si deve fare clic sull'icona a forma di ruota dentata in basso a destra. Da qui possiamo fare tutte le varie modifiche, compreso il cambio Nick, l'impostazione dei proxy e altro ancora.



Da qui possiamo scegliere se unirci a una rete esistente o crearne una nostra.

:: Utilizzo di Hamachi

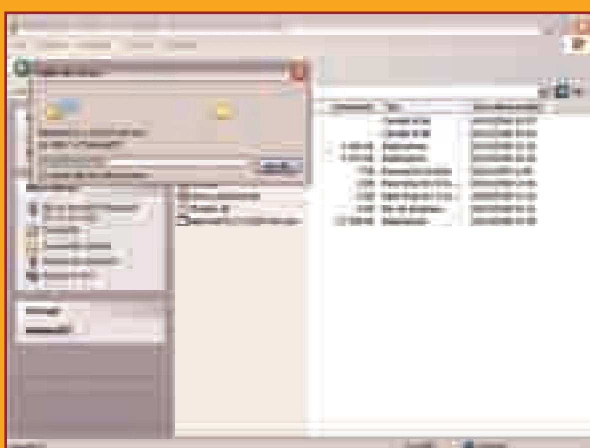
Dopo aver personalizzato tutte le varie funzioni, facendo clic sul pulsante in basso a sinistra sarà possibile accedere alla rete. Appena verrà ottenuta la connessione il sistema mostrerà in altro l'indirizzo IP della scheda di rete virtuale di Hamachi. Questo indirizzo verrà usato per accedere a reti Hamachi già esistenti oppure per creare la nostra rete privata. Il consiglio è quello di configurare subito una master password, quindi creiamo la nostra rete o connettiamoci a una esistente facendo clic sull'icona con il triangolo in basso a destra. Una volta stabilita la connessione con il server è possibile verificare anche il traffico generato dalla rete aprendo Risorse di rete e facendo doppio clic sulla scheda di rete Hamachi.
Se creiamo noi la rete, dopo aver comunicato ai nostri amici il nome della stessa e la password che abbiamo scelto, sarà possibile utilizzare i veri servizi del programma. Il più immediato è quello di chat, in realtà semplicissima ma molto utile se si stanno condividendo file o cartelle e si vuole contattare direttamente l'utente senza dover usare altri messenger. In modo altrettanto semplice si può avviare una sessione di ping continua facendo doppio clic sul nome dell'utente destinatario. È molto utile se vogliamo cercare di capire se c'è qualche problema di performance sulla rete. Per trovare invece i nostri "vicini di rete" possiamo usare sia Risorse di rete facendo clic su Cerca computer... sia dal menu contestuale di Hamachi selezionando Cerca.Una volta ottenuta la connessione diretta con il PC del nostro amico, possiamo mandare e ricevere file semplicemente usando le condivisioni di Windows, come se si stesse lavorando su una rete locale. Infinitamente più veloce che con qualsiasi programma P2P.



La chat di Hamachi, spartana ma veloce e molto utile.

:: Il vero scopo di Hamachi

Hamachi in realtà nasce come protocollo di comunicazione per poter giocare in multiplayer anche se non si è collegati alla stessa rete locale. Con un po' di pazienza si può configurare la rete per l'utilizzo con la maggior parte dei giochi. In questo caso si potrebbero verificare dei problemi dovuti al fatto che alcuni server giochi richiedono che i giocatori si trovino sulla stessa rete. Mi spiego meglio. Prendiamo per esempio gli IP 5.1.12.123 e 5.1.34.111 . In questo caso non ci dovrebbero essere problemi. Ma la rete di Hamachi difficilmente assegnerà IP vicini ai vari utenti, quindi sarà molto facile un che il secondo IP sia 5.4.21.145 e, in questo caso, il server potrebbe dare un errore del tipo "IP Class C error". Niente paura, sarà facile risolvere il problema facendo clic destro sul nostro amico presente in elenco e assegnargli un "Peer VPN alias" che si addica alle nostre esigenze.



I trasferimento di file avviene direttamente via condivisione di Windows.

:: Conclusioni

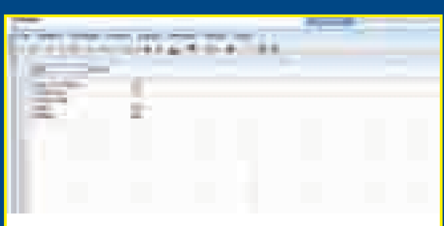
Il sistema di connessione offerto da Hamachi è molto utile per creare piccole network VPN e ha il vantaggio di essere molto leggero e sicuro utilizzando il protocollo SSL. Bisogna però stare attenti a quando si configurano opzioni di connessione con bridging perché si potrebbero modificare involontariamente le impostazioni di rete correnti e rendere inutilizzabile la rete locale o Internet per alcune applicazioni. Nel complesso l'impressione è di avere una rete rapida e semplice che permette di agire sui computer dei nostri amici un po' come se fossero a casa nostra.

Niente P2P ma vero e proprio utilizzo di software direttamente dalla Rete. Se ne parla da tanto tempo, facciamo il punto



ALLA RICERCA DEL SOFTWARE CONDIVISO

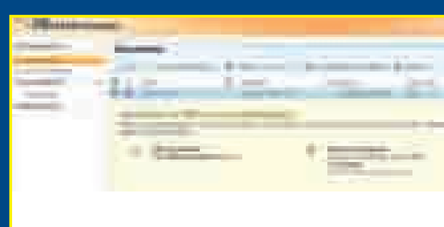
Ne parlò zio Bill già parecchi anni fa recitando, più o meno, così " a breve (il breve di Microsoft ovviamente) i programmi non gireranno più sui singoli PC ma su server centralizzati a cui gli utenti accederanno via Internet". Il tempo passa e i software li installiamo ancora, sempre invadenti e sempre più pesanti, ma la strada è stata davvero intrapresa e i segnali sono molti e cominciano ad essere ben visibili. Basti pensare ad Azure, il kernel del futuro sistema operativo di casa Microsoft pensato per operare interamente su Internet. E anche sul fronte programmi online si sono mossi passi da gigante tanto che oggi, in presenza di una buona connessione, è possibile fare a meno di un pacchetto office installato sul nostro computer e lavorare senza alcun intoppo. Anzi, a dircela tutta con parecchi vantaggi, primo fra tutti quello di avere i nostri documenti sempre pronti per essere letti e modificati in qualunque angolo del mondo ci troviamo. Ma andiamo con ordine e iniziamo dalla nuova mamma di tutti gli internettomani: Google.



L'interfaccia dei vari strumenti è molto intuitiva : il foglio di calcolo è praticamente identico a Excel e ha tutti gli strumenti di necessari per lavorare.

:: Google documenti

Il primo plus del servizio appare immediatamente: si accede con l'account di Gmail, lo stesso con cui si può accedere ai servizi "Foto" e "Calendar". Le funzioni che offre sono quelle di un pacchetto office classico, quindi word processor, foglio di calcolo e presentazioni. Sono disponibili tutti gli strumenti per la formattazione, e nel caso del foglio di calcolo le formule, per creare ed elaborare file come se stessimo lavorando con Office di Microsoft o con OpenOffice. Come detto precedentemente però, possiamo farlo da qualunque computer e su qualunque piattaforma, sia essa Windows, Mac o Linux. Lo spazio per poterli salvare online è quello immenso di GMail. Le uniche limitazioni sono i 500Kb di peso per i documenti Word ed Excel e 10Mb per le presentazioni.



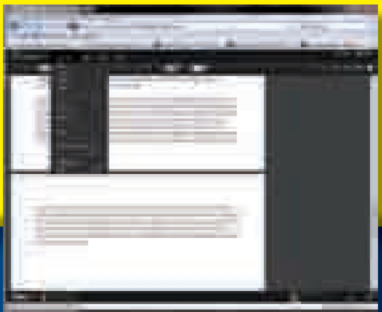
Già dall'interfaccia, solo in inglese, si capisce la sua natura: carica e condividi.

EDIT PAD

È un editor testi ultra basico, solo testo senza fronzoli. Scrivi e salvi sul computer. Ci sono alcuni gadget come il conteggio delle parole (ma sbaglia il conteggio).
Perché usarlo se fa le stesse cose di NotePad o dell'equivalente nei vari sistemi operativi? Perché vuoi mettere la figura quando ti metti al computer della ragazza di turno e digiti su un fondo giallo in puro stile hacker?
http://www.editpad.org/

ACROBAT.COM

Stiamo parlando di Adobe, quindi di un'azienda sul livello, o quasi, dei due giganti. La proposta del papà di Acrobat e Photoshop presenta un editor di testi completo di tutte le funzioni di editing tipiche di un programma commerciale come Word. L'interfaccia grafica è in Flash; forse non è il massimo dal punto di vista dell'organizzazione funzionale ma ha davvero tutto e nel complesso gira abbastanza veloce, a patto ovviamente di avere una connessione accettabile(stiamo pur sempre lavorando on line). Infine offre la funzione di storage dei file fino a 5 gb e la condivisione dei documenti con altri utenti registrati. La conversione degli stessi nel formato pdf è invece solo una demo del programma commerciale.
www.acrobat.com



Google Documenti viene presentato come versione Beta, ma è abbastanza solido in quanto derivato di un noto software sviluppato da Writely, ormai acquistata dal colosso americano.

:: La risposta di Microsoft

Microsoft del resto non è rimasta a guardare e ha ulteriormente sviluppato il suo strumento: Office Live Workspace. Si tratta di una suite di applicazioni in apparenza simili a quelle proposte da Google, in realtà con una grande differenza: per visualizzare la suite di Google non serve altro che un browser aggiornato, mentre per visualizzare al meglio i servizi Microsoft si deve installare SilverLight (stupefacente se pensiamo che la strada ai programmi online l'ha lanciata proprio Gates, non se pensiamo alla nota propensione di Microsoft a controllare il controllabile) Inoltre Office Live Workspace è fondamentalmente uno spazio nel quale possiamo parcheggiare i nostri documenti, mentre le operazioni di editing dei documenti è ridotta all'osso: praticamente copia e incolla.

:: Il resto del mondo

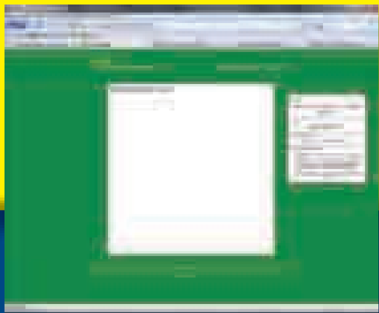
Già perché, incredibile per molti ma non per noi, Internet non è solo Google e Microsoft. Anzi, il meglio spesso si cela proprio tra le pieghe dei servizi e prodotti Open Source. Ecco quindi una selezione di servizi online, tutti rigorosamente gratuiti.

NUM SUM

È un Foglio di calcolo abbastanza completo, dal punto di vista funzionale quasi a livello di quello offerto da Google. Permette di importare dati da un file txt tabulato, aprire un foglio Excel ed editarlo (ma in questo caso abbiamo incontrato parecchi problemi) o crearne uno nuovo. I file possono essere archiviati online o esportati in vari formati tra cui la pagina web.
http://numsum.com

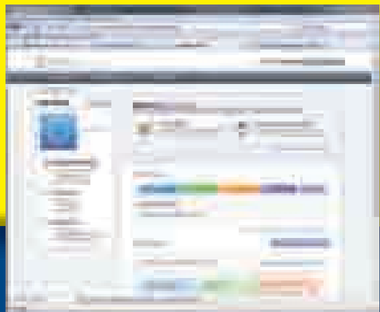
POTE

Un passo più avanti di Edit Pad. Ci si registra (gratuitamente) e si possono salvare fino a 25 file sul loro server, che avremo sempre disponibili ovunque ci troviamo. Qualche piccola possibilità di formattazione, poca cosa ma quanto basta per differenziare linee e commenti. Veloce e affidabile, un'ottimo strumento per prendere appunti e non rischiare di perderli. Ideale per il vero hacker.
www.pote.com



MY OFFICE

Ha le stesse funzioni di Google Documenti, da Word a Excel a Power Point. Possiamo archiviare i nostri file online fino a 1 gb per poterli aprire ed editare ovunque ci troviamo o condividerli con altri colleghi e amici. Utile la funzione per sincronizzare una o più cartelle del nostro computer con l'archivio online. L'interfaccia è pensata anche per utenti meno esperti, semplice da usare e gradevole nell'aspetto ma paga qualcosa in termini di velocità.
http://www.thinkfree.com/





CASSEFORTI PORTATILI

Facciamo una panoramica su quanto di portatile e sicuro ci offre oggi la tecnologia

Un tempo esisteva la cassaforte dove riponevamo i documenti importanti, poi siamo entrati nell'era digitale e i documenti abbiamo iniziato ad archiviarli in aree protette del PC: file compressi protetti da password, dischi virtuali criptati, ecc... Oggi spesso e volentieri li teniamo su una chiavetta USB per averli sempre con noi. Pratico sì ma rischioso, basta che ti scivoli dalla tasca et voila... chiunque la trovi può accedere a quanto vi abbiamo salvato. Vediamo un po' quali nuovi "gadget" abbiamo a disposizione per evitare che i nostri segreti finiscano in vetrina.

:: Storage sicuro

Uno dei dispositivi per la conservazione dei dati più facile da trovare e da usare è, appunto, la classica chiavetta USB. Sono talmente economiche che oggi vengono offerte da alcune aziende come omaggio e sono disponibili anche con capacità interessanti, in grado di contenere l'equivalente di diversi DVD di dati. Kingston produce DataTraveler Secure, una chiavetta dalle caratteristiche di sicurezza adeguate: dispone infatti di un sistema di cifratura AES basato su hardware con chiave da 256 bit. Non è proprio economica, quella da 8 GB costa infatti intorno ai 250 dollari, ma se la nostra priorità è la sicurezza dei dati, il prezzo non dovrebbe essere un problema. E possiamo alzare ancora il livello di protezione (e il prezzo) optando per la chiavetta USB IronKey. Anch'essa basa la propria sicurezza su un chip interno che si fa carico del lavoro di autenticazione e di cifratura dei dati, ma in più dispone di un browser Web integrato (per la precisione si tratta di Firefox) per accedere all'account personale my.ironkey.com, da cui si gestiscono i propri dati (sia i nostri documenti sia quelli di autenticazione).

Inoltre i suoi standard costruttivi comprendono corpo in metallo impermeabile e resistente, personalizzato con un codice univoco e ulteriormente personalizzabile con un codice scelto da noi, in modo da essere riconosciuta in caso di furto. Anche in questo caso i costi sono abbastanza elevati, arrivando intorno



DataTraveler Secure, prodotta da Kingston, protegge i dati automaticamente.



Con la chiavetta proposta dall'indistruttibile IronKey i dati sono protetti con un account online accessibile dal browser Firefox integrato.

ai 300 dollari per la versione base personale da 8 GB(sì solo 8 GB ma… impenetrabili).
Se invece non disponiamo di budget così elevati (e in questo periodo di crisi probabilmente pochi hanno questa fortuna), possiamo rivolgerci al software open source per ottenere un risultato simile: TrueCrypt è un ottimo programma di cifratura gratuito e disponibile per diverse piattaforme che possiamo usare per cifrare file, partizioni o interi dischi, compresi quelli USB. Naturalmente per poter accedere ai nostri dati avremo bisogno di installare il programma su tutti i PC a cui colleghiamo la chiavetta di memoria.

:: Doppia password

Un discorso particolare merita la soluzione offerta da Refog.com. Si tratta di un software che può essere installato su qualunque supporto USB che disponga di almeno 2 MB di spazio libero. Quando inseriamo il supporto scelto nella presa USB del computer, questo programma parte automaticamente e intercetta qualunque password inseriamo, trasformandola in una password molto più complessa e difficile da ricordare e da indovinare. In questo modo possiamo anche continuare a usare normali password "semplici", in quanto anche se queste vengono indovinate da un malintenzionato non potranno funzionare se la nostra chiavetta USB non è collegata ai nostri PC, di fatto proteggendo tutto ciò che si trova al di là della password.

:: Autenticazione

La classica chiavetta USB può essere usata non solo per conservare dati sicuri, ma anche come vera e propria chiave di accesso. Per questo scopo però non basta una comune chiavetta di memoria ma occorre che, come quelle appena presentate, contengano chip di cifratura e protezione adatti. Il software installato sul computer da questi dispositivi, invece di chiedere solo una password (comunque presente), si assicurerà che la chiavetta speciale sia inserita in una porta USB prima di permettere l'accesso ai dati protetti. La stessa tecnologia può essere adottata (e in effetti lo è, pensiamo per esempio al classico Bancomat o alla carta di credito) anche via Smart Card o altri supporti, e addirittura su floppy o su CD.

La porta USB del PC può ospitare anche altri dispositivi di sicurezza. Sta diventando molto comune il lettore di impronte digitali, grande come una chiavetta di memoria e in grado di permettere solo a noi l'accesso al PC. Tra i principali produttori di questo dispositivo troviamo Lenovo, che lo incorpora in molti dei propri notebook. Esiste anche chi ha unito le due cose: lettore di impronte digitali e chiave di memoria. Lo ha fatto Transcend con i prodotti JetFlash 220 Fingerprint. Questa chiavetta, che si apre a compasso, offre un valido supporto di memorizzazione abbinato a un sistema di autenticazione a impronte digitali, praticamente inviolabile!



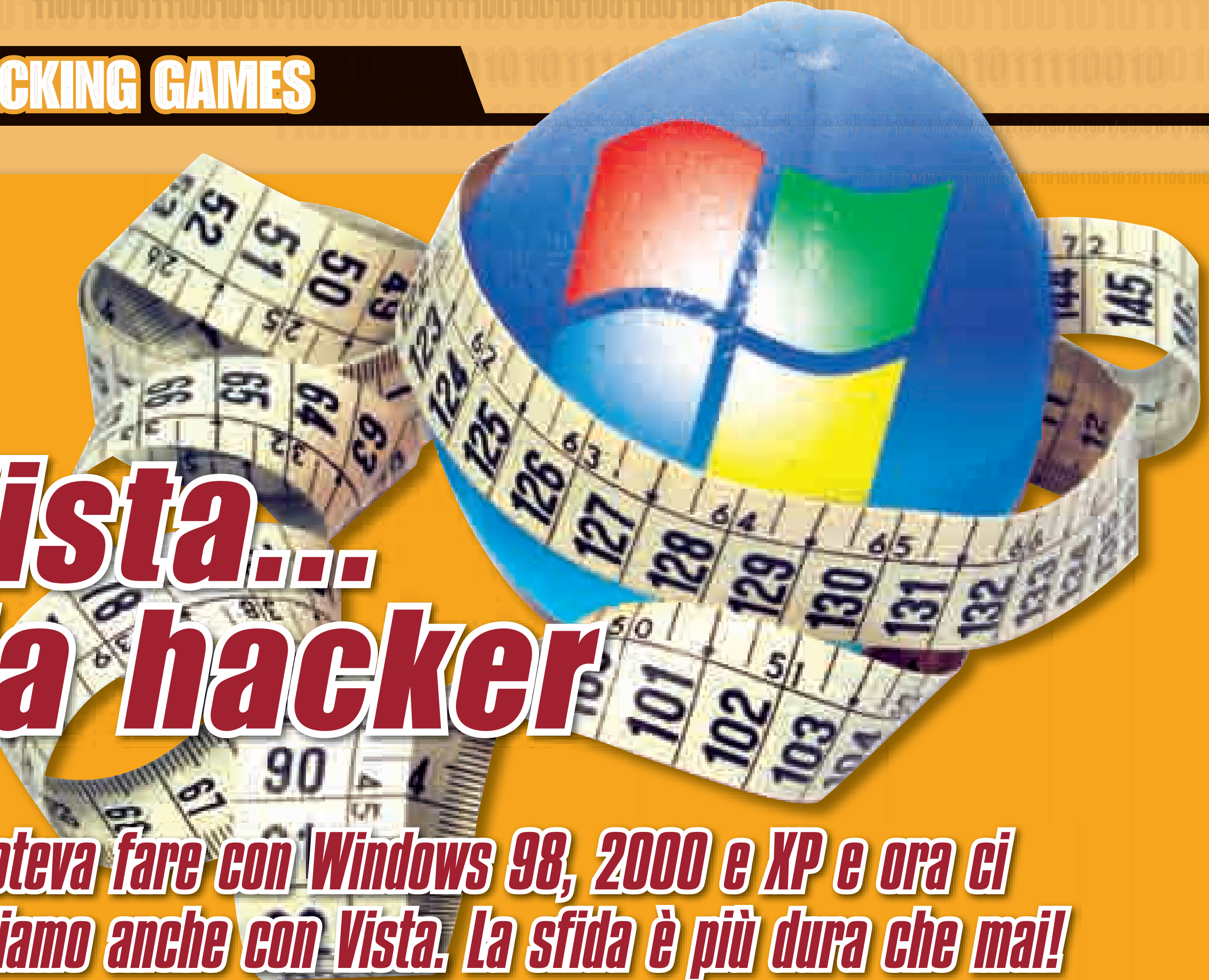
Jet Flash 220 Fingerprint è una chiavetta USB che integra un lettore di impronte digitali.

:: Chiave digitale

Esiste anche un progetto amatoriale che intende usare una chiavetta USB come se fosse una normale chiave per serrature: naturalmente si tratta di una serratura elettronica pilotata da PC. È un progetto che chiunque abbia un minimo di dimestichezza con l'elettronica e il saldatore può costruirsi. Il principio si basa sul fatto che ogni chiavetta USB ha un proprio codice seriale implementato direttamente nell'hardware della stessa. Leggendo questo codice e confrontandolo con quelli contenuti in un database, è possibile verificare se chi ha inserito la chiavetta è autorizzato ad accedere all'area protetta oppure no.
Se è autorizzato, cioè se il codice della chiavetta è presente nel database, il PC apre una serratura elettromeccanica per mezzo di un controllore.
Il progetto di questo dispositivo, che si basa su un microcontrollore Arduino di facile reperibilità, lo possiamo trovare all'indirizzo https://256.makerslocal.org/wiki/index.php/USB_Auth ed è basato su Linux, ma è facilmente adattabile (da chi sa programmare un po') per altre piattaforme.



Questa serratura elettromagnetica realizzata amatorialmente si apre solo se si collega una chiavetta USB autenticata.



Vista... da hacker

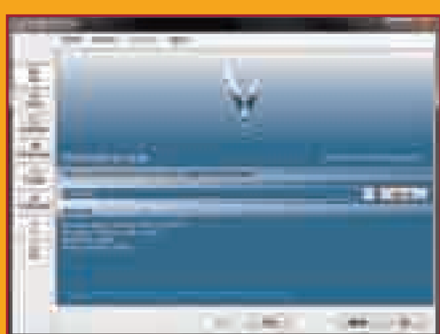
Si poteva fare con Windows 98, 2000 e XP e ora ci proviamo anche con Vista. La sfida è più dura che mai!

Windows Vista è stato un deciso passo indietro rispetto alle ultime versioni di Windows XP, probabilmente il prodotto più apprezzato di casa Microsoft e probabilmente sparirà presto dalla memoria di molti non appena arriveranno le nuove versioni. I motivi di questo scarso successo sono molteplici e ognuno ha un proprio parere sul suo (poco) appeal. Tuttavia questo è il sistema operativo che, con molta probabilità, troviamo preinstallato acquistando un nuovo PC, pertanto dobbiamo un po' adattarci. Adattarci non significa arrenderci, e come già sperimentato con Windows XP, proviamo a "ritoccarlo" creandone una versione strip down.

:: Poco versatile

Il problema principale dell'operazione che vogliamo effettuare sta nel fatto che la versatilità non è il suo forte. Molti smanettoni in tutto il mondo stanno provando a mettere a punto un'installazione ridotta di Vista, ma prima o poi salta fuori qualche problema che di fatto lo rende inutilizzabile. Non ci troviamo, quindi, nelle stesse condizioni di un'installazione di XP che, grazie a XPLite, era possibile ridurre addirittura a 40 MB lo spazio occupato e a sistema operativo già installato, o ai soli 9 MB necessari per un Windows 9x embedded!

In questo caso possiamo rimuovere alcune funzionalità non critiche, ma non abbastanza per poter affermare di averlo realmente ridotto ai minimi termini.

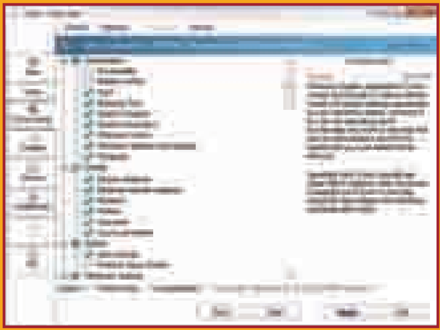


La prima schermata di vLite ci chiede dove trovare i file originali di Vista e dove salvare i file necessari per la nuova ISO.

Inoltre, questa operazione è possibile solo prima di aver installato il sistema stesso, cioè agendo sui file di setup e ricreando un'immagine ISO dell'installazione pronta per essere usata su un nuovo PC. Il programma da usare per compiere questa operazione si chiama vLite ed è disponibile all'indirizzo http://www.vlite.net/.

:: Cosa serve

Innanzitutto ci serve il supporto originale su cui è presente l'installazione di Vista. Da lì il programma recupera i file necessari in base alle opzioni che abbiamo scelto e li masterizza di nuovo su DVD (parlare di CD come per XP in questo caso è proprio impossibile) con il file contenente lo script di installazione modificato. È di fatto l'erede di nLite, il programma con cui potevamo creare versioni versione strip dow dei precedenti S.O., ed è importante notare che non dobbiamo per forza eseguirlo su Vista: se disponiamo del DVD originale possiamo preparare l'immagine anche usando Windows XP.



L'elenco delle opzioni che si possono rimuovere. Per quelle vitali, viene mostrato un avviso come questo.

Per creare l'immagine finale abbiamo bisogno anche di almeno 4 GB di spazio libero su disco.

:: Come procedere

Installiamo vLite sul nostro PC e inseriamo il DVD originale di Vista nel lettore del nostro PC. Dopo aver avviato il programma e accettato le condizioni d'uso, dobbiamo selezionare l'origine dei file di Vista, cioè indicare a vLite il drive in cui risiede il DVD originale e in un paio di minuti (dopo che il programma avrà compiuto la lettura e la preparazione dei file iniziali) potremo iniziare a spulciare tra le varie opzioni per risparmiare un po' di spazio.
Le opzioni che il programma permette di rimuovere sono davvero tante. Passando il puntatore su ognuna di esse ne potremo leggere una descrizione sul pannello di destra e un avviso ci avvertirà se il componente in questione è vitale per il funzionamento di altri componenti. In questo caso dovremo pensarci bene prima di rimuoverlo, pena il malfunzionamento del sistema operativo una volta installato. A titolo d'esempio, ecco gli elementi che la comunità online è riuscita a individuare come rimovibili senza particolari problemi:

GAMES
- Inbox Games
- Premium Inbox Games

HARDWARE SUPPORT
- SmartCards

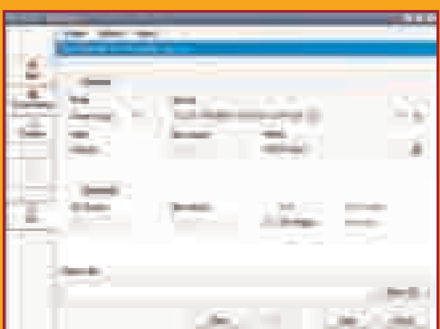
LANGUAGES
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

MULTIMEDIA
- Speech Support
- Tablet PC
- Wallpapers

NETWORK
- Connect to a Network Projector
- Internet Information Services
- Remote Desktop and Assistance

SERVICES
- Error Reporting
- Remote registry
- Windows Remote Management

SYSTEM
- Accessibility
- Natural Language
- Windows Easy Transfer



La fase di masterizzazione del nuovo DVD di Vista con l'installazione minimale.

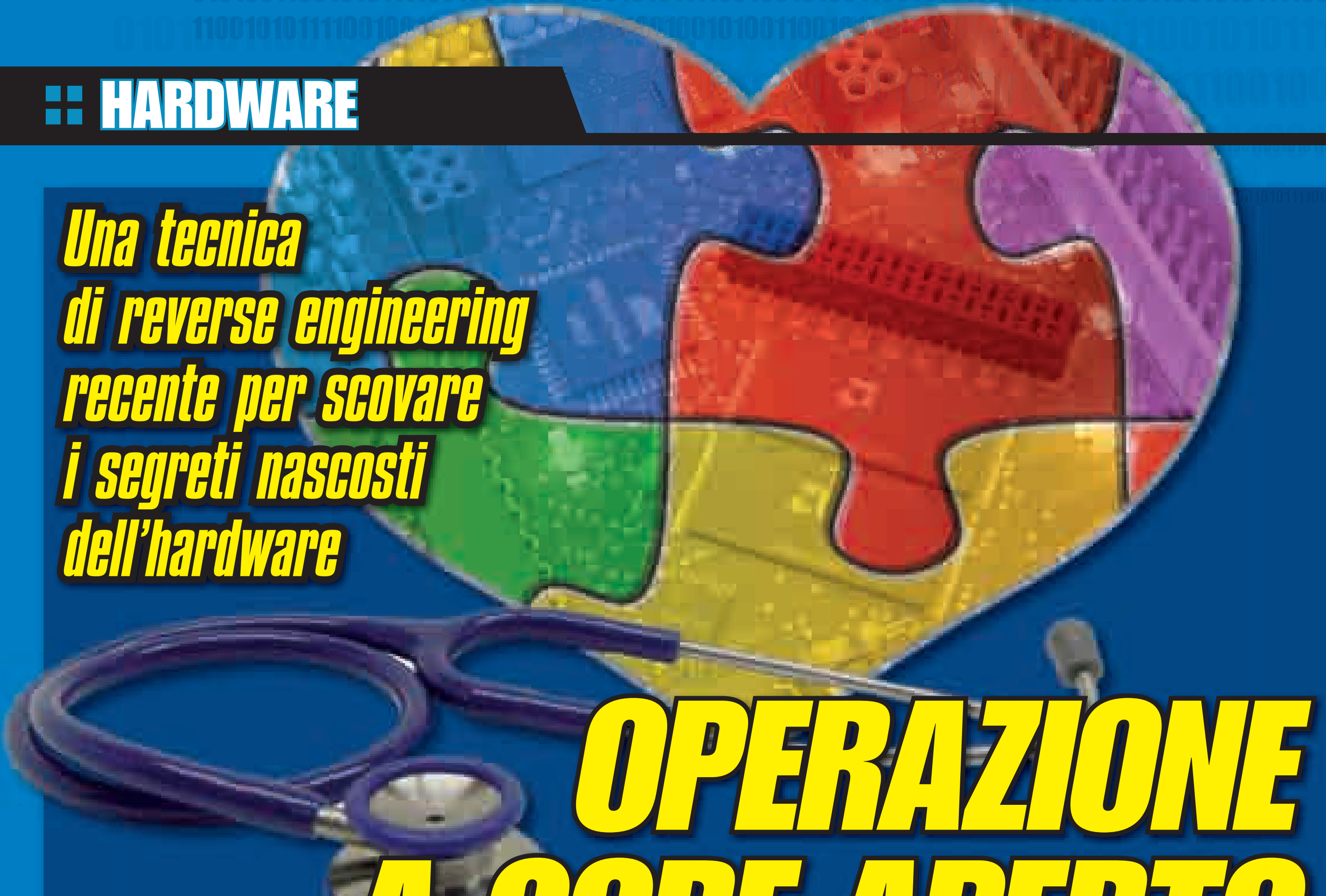
Dopo aver selezionato quelli che ci interessa rimuovere, facendo clic su Next accediamo alla fase di creazione della ISO finale. Possiamo scegliere se rimuovere completamente i file non necessari dalla nuova versione ridotta, oppure mantenerli lo stesso e modificare solo quelli con gli script di installazione perché non li considerino e non li copino sul disco in fase di setup. Non ci resta quindi che masterizzare la nostra personale versione di Vista e provare a installarla su un PC o su una macchina virtuale per vedere se funziona.
I vantaggi principali di una versione ridotta con vLite di Windows Vista sono sostanzialmente in termini di spazio occupato su disco, non tanto di prestazioni. Rimuovendo praticamente tutti i componenti sicuri menzionati si possono risparmiare alcune centinaia di MB (neanche tanto dato che Vista completo può occupare anche 15 GB di spazio su disco!). Qualcuno sui forum online afferma di aver ridotto l'installazione fino a 1,5 GB, ma non è dato sapere con quale affidabilità e usabilità. Avremo anche qualche programma in meno che gira in background, ma per avere veramente un incremento in termini di prestazioni il parere è unanime: disabilitare Aero, l'interfaccia grafica di Vista, dal menu Personalizza per passare a quelle più spartane fino a raggiungere quella ultra leggera derivata da Windows 2000.

:: Altre opzioni

In realtà vLite ci permette di compiere anche altre operazioni, ma per ora non sono affidabili al 100%. Per esempio, possiamo integrare nell'installazione eventuali driver per periferiche in nostro possesso, oppure includere service pack e aggiornamenti pubblicati da Microsoft nel corso del tempo. Possiamo anche includere altro software di cui vogliamo disporre a installazione ultimata. In questo caso però non ci troveremmo davanti a una versione ridotta di Windows Vista ma, al contrario, andremmo ad aumentarne le dimensioni considerevolmente.
Le altre opzioni disponibili permettono di impostare gli script di installazione in modo che questa avvenga completamente unattended, cioè senza alcun intervento da parte nostra, nemmeno per l'inserimento del codice prodotto.

:: Qualche alternativa?

Dire "passiamo a Linux" è troppo scontato, qui si sta parlando proprio di continuare a usare Vista ma solamente con i componenti essenziali al suo funzionamento. Esiste in Rete una versione ridotta all'osso di Vista chiamata TinyVista e scaricabile via Torrent che promette di installarsi in meno di 3 GB di spazio, di funzionare anche con soli 256 MB di RAM e di mantenere sia Aero sia i programmi principali come Internet Explorer 7 e Windows Media Player. Si tratta di un prodotto non ufficiale, dato che permette l'installazione senza chiedere alcun codice prodotto: attenzione a quello che scaricate...



Una tecnica di reverse engineering recente per scovare i segreti nascosti dell'hardware

OPERAZIONE A CORE APERTO

Reverse engineering significa in soldoni smontare le cose per vedere come funzionano; l'abbiamo fatto tutti da piccoli con i nostri giocattoli e alcuni di noi continuano a farlo con giocattoli ben più costosi. Dai cinesi che, negli Anni '60, arrivavano in Italia e smontavano le penne biro per poi riprodurle in patria, la filosofia di base non è cambiata ma sono cambiati i metodi e gli oggetti di studio. E, naturalmente, gli scopi.

:: Perché il reversing

Per capire come funziona una cosa possiamo agire in due modi: affidarci al manuale tecnico, se esiste e se è ben dettagliato, oppure smontarla pezzo per pezzo e capire lo scopo di ognuno di essi e come interagiscono tra loro. È facile a dirsi se si tratta di un semplice giocattolo o di un oggetto con relativamente pochi pezzi; diventa già più difficile se entriamo nel mondo dell'elettronica o, peggio, dell'informatica.

Innanzitutto bisogna avere delle conoscenze almeno di base della tecnologia dell'oggetto che stiamo studiando: dobbiamo riconoscere in un tostapane l'alimentatore, il timer e l'elemento riscaldante, che sono i tre blocchi principali che lo compongono. In questo modo possiamo dire, dopo averlo esaminato, che l'alimentatore mantiene in temperatura l'elemento riscaldante finché il timer non conta il tempo impostato.

Se, quindi, conosciamo i "mattoni" che compongono un oggetto, diventa abbastanza semplice intuire (è questa la parola giusta) quale sia il suo funzionamento. Ma sapere come funziona il tostapane non è molto utile, lo sappiamo già.



Un comune integrato PIC dopo aver eroso il rivestimento esterno per mettere in vista il chip di silicio.

Ecco quindi il perché del reverse engineering, o reversing detto in breve: per capire a cosa serve e come funziona un oggetto che non conosciamo.

:: I campi di utilizzo

Principalmente il reverse engineering è applicato quotidianamente in campo industriale: inutile nascondersi dietro un dito, se un concorrente fa qualcosa meglio di una certa azienda, questa si procurerà subito uno di questi oggetti, lo smonterà, lo studierà e cercherà di carpirne i segreti per adeguare la propria produzione.

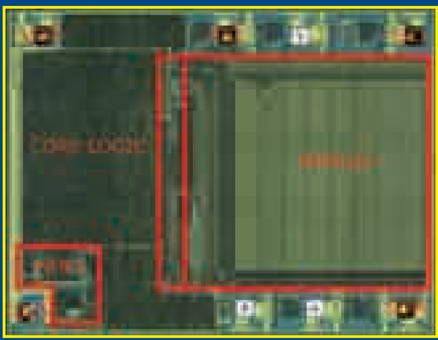
Un altro campo di utilizzo del reversing è l'ambito militare. Se l'esercito del Paese X riesce ad appropriarsi (rubandola con le spie o entrandone in possesso fortunosamente per esempio per un incidente che fa precipitare un caccia sul proprio territorio) della tecnologia del nemico, non aspetterà un secondo per studiarla e trarne le appropriate contromisure (o dotarsi della stessa tecnologia se migliore della propria).

Ma dato che al giorno d'oggi praticamente tutto è basato sull'elettronica e sui

computer, non basta più, diciamo così, smontare il tostapane, si deve entrare più a fondo nella natura delle cose.

:: Chip reversing

Oggi l'elettronica non è più quella di una decina d'anni fa. È uno dei campi in cui il progresso tecnologico corre molto velocemente e in cui non si fa a tempo ad adeguarsi a un nuovo dispositivo che già è in circolazione una versione migliorata. Di questo passo, un'azienda moderatamente dotata di fondi e di risorse tecnologiche non si basa più su altre tecnologie esistenti, ma è in grado di crearsi i propri chip in casa.



Un comune integrato PIC dopo aver eroso il rivestimento esterno per mettere in vista il chip di silicio.

Qui le cose si fanno difficili: possiamo vedere una basetta elettronica con uno o più chip, che magari non riportano nemmeno sigle o diciture sul corpo e quindi non ci permettono di identificarli, pertanto il reversing della basetta risulta praticamente impossibile. Finora. Esiste infatti una nuova tecnica (che, come dicevamo in apertura, non è appannaggio di tutti) che permette, previa distruzione del chip stesso, di capirne il funzionamento e quindi di riprodurlo con altri mezzi. Premettiamo una cosa: non tentate di farlo in casa. Per aprire il corpo di un chip non basta agire con un taglierino, perché il chip di silicio è annegato nella plastica stessa del corpo. Bisogna usare acidi pericolosi che nessuno probabilmente ha in casa e che si trovano solo in laboratori chimici. Inoltre, date le ridotte dimensioni del wafer di silicio, occorrono apparecchiature per ingrandire e fotografare, che di solito sono molto costose e comunque difficili da costruire in modo amatoriale.

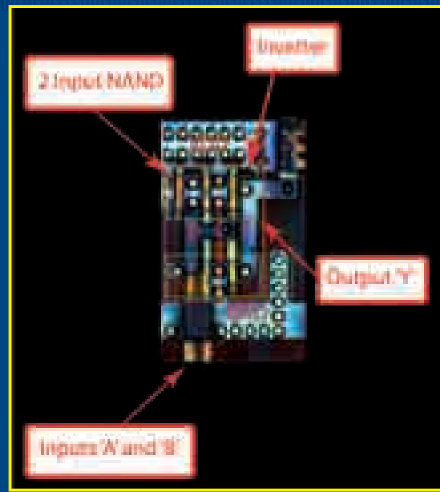
:: Lo studio di un chip

La prima cosa da fare è ovviamente liberare il supporto di silicio dalla plastica del corpo, per mezzo di acidi speciali che non intacchino l'oggetto della ricerca ma solo la plastica che lo racchiude. Una volta esposto, bisogna porre il chip sotto le potenti lenti di un microscopio in grado di ingrandire l'immagine di almeno 500 volte e collegato a una fotocamera digitale ad alta risoluzione. Illuminando il chip con luce non diretta (questo perché la luce diretta è troppo forte e non permette di riconoscere a vista gli elementi che compongono il chip), si scattano diverse fotografie della parte interessata, che poi vengono composte in un'unica immagine ad altissima risoluzione. Su questa poi viene fatto lo studio vero e proprio. Come già detto, occorre avere le cognizioni di base per poter fare il reverse engineering di un chip di silicio. Bisogna cioè saper riconoscere come un transistor o un qualsiasi altro componente elettronico viene riprodotto a livello molecolare su un chip, perché alla fine di questo si tratta. Studiando quindi la configurazione dei componenti elettronici microscopici che lo compongono

FARLO PER GIOCO

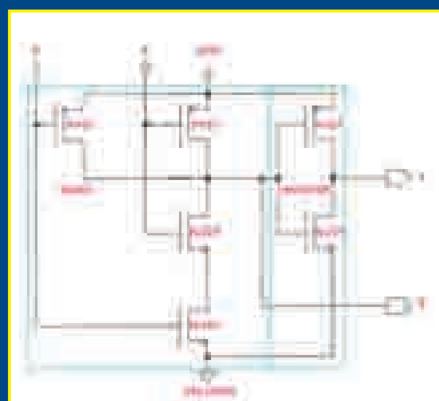
Un ingegnere elettronico con il pallino dei videogames è riuscito a creare divertenti trasposizioni di una tecnica simile: in Ruckingenur e Ruckingenur II dobbiamo reversare delle basette elettroniche soffiate a un esercito nemico. Su www.zachtronicsindustries.com troviamo questi e altri giochi a sfondo ingegneristico.





Un blocco viene scomposto in ulteriori sottoblocchi per individuare i singoli circuiti che lo compongono.

e i collegamenti tra loro si è in grado di capire di che circuito fanno parte: un oscillatore, una cella di memoria, una porta logica e così via. Ricreando quindi il circuito in un programma di simulazione come Multisim di National Instruments (costoso e complesso), si è in grado di stabilire a cosa serve ogni singolo circuito trovato nel chip.



Dai sottoblocchi si ricava uno schema elettrico che viene dato in pasto a un programma come Multisim per la simulazione.

Con questo sistema alcuni ricercatori sono già riusciti a "craccare" il circuito di un chip RFID (che pertanto potrà essere replicato, con somma gioia di chi vorrà rubare soldi usando i metodi di pagamento e riconoscimento a prossimità) e il chip di una Smart Card, come quello contenuto in una carta di credito.

Trinity 82

LUCCHETTI DIGITALI

Protezione digitale dei diritti di autore o sopruso delle Major?

Il bello del digitale è che puoi copiare le informazioni all'infinito ottenendo una copia indistinguibile dall'originale. Questa caratteristica unica è stata però la rovina di quanti sull'unicità di un prodotto hanno basato il loro business: basti pensare ai produttori di videogiochi o i produttori di materiale audio o video.

:: Cosa sono i DRM

Per limitare o almeno rendere difficile la possibilità di copiare un film o un gioco sono stati realizzati dei meccanismi digitali che prendono il nome di Digital Right Management (DRM), gestione dei diritti digitali. Il loro scopo principale è quello di permettere ai titolari dei diritti di esercitare un controllo sulle proprie opere una volta distribuite. Questo controllo permette di proteggere, identificare e tracciare il prodotto che viene criptato con DRM. Forse il più famoso sistema realizzato è stato il Content Scrambling System (CSS, letteralmente sistema di disturbo del contenuto) impiegato per cifrare il contenuto dei DVD, ma anche il sistema Macrovision (tuttora impiegato nei videoregistratori e nei player DVD) per impedire la copia non autorizzata.

:: Come funzionano

Alla base del funzionamento dei DRM c'è la crittografia, cioè la possibilità di trasformare il contenuto "in chiaro" in un contenuto leggibile solo conoscendo una chiave di cifratura di cui si è in possesso se si è legittimi fruitori del contenuto. Questo meccanismo ha il suo punto debole proprio nella chiave: se si decritta, viene automaticamente reso libero il contenuto, che d'altronde non può essere letto nella forma cifrata.
Sono stati via via implementati algoritmi sempre più complicati che permettono diversi livelli di sicurezza, ma è bene ricordare che nessuno di questi offre una garanzia a vita (basti pensare al crack del WPA2, vedi HJ165). A ogni modo con sistemi di cifratura a doppia chiave (tipo il PGP) il grado di sicurezza aumenta perché occorrono entrambi le chiavi per decifrare il contenuto, mentre nei DRM la chiave è una sola.
C'è un'altra debolezza dei DRM: chi cifra il contenuto (produttore) ha interesse che tale contenuto sia comunque



fruibile, anche se vuole esercitare il suo controllo. Per quanto riguarda il CSS, la chiave di decrittazione è stata quindi distribuita ai produttori dei player. In questo modo un lettore di DVD (software o hardware) è in grado di leggere il contenuto cifrato di un DVD regolarmente acquistato, ma possiede al suo interno una chiave che dovrebbe restare segreta per assicurare la sicurezza della protezione. Nel caso del CSS non è stato così (vedi il caso di DVD Jon). Ma la debolezza è intrinseca: nel momento in cui il dato viene messo in chiaro, ad esempio per la visione del film, è possibile salvare il contenuto ed eliminare quindi la protezione.



DVD Jon, al secolo Jon Lech Johansen, è forse il più famoso cracker mondiale attivo già dal 2002.

Se aggiungiamo che grazie a Internet è possibile trovare soluzioni che superano queste protezioni, viene il dubbio che il DRM sia del tutto inutile. In realtà l'idea alla base del DRM è che renda meno facile la copia libera dei contenuti anche se ne siamo i legittimi proprietari.
E da qui la protesta in tutto il mondo, contro quello che è stato giudicato a più riprese come un vero sopruso da parte delle major e dei finanziatori (tra cui Microsoft) di questi sistemi di protezione. In Europa poi la normativa dei singoli stati prevede la legittimità di produrre una copia di riserva per uso privato e in diverse occasioni il DRM impedisce e quindi limita questo diritto individuale. Non solo: se la licenza di visione di un contenuto video viene concessa solo se utilizzo un software Microsoft (Windows Media Player), non posso neanche accedervi se utilizzo Linux!

IL PROGRAMMA CHE CI LIBERA

Supponiamo di aver acquistato legittimamente una canzone in formato WMA che vogliamo ascoltare poi sul nostro player WMA/MP3. Proviamo a copiare il file e non riusciamo ad ascoltare nulla. Perché? Il distributore del contenuto ha inserito il DRM nel file e la chiave per decrittarlo è contenuta nel PC in formato cifrato. Viene in aiuto un simpatico tool freeware chiamato FairUse4WM, che leggendo la chiave realizza una copia in chiaro del file che possiamo poi finalmente ascoltare sul nostro player portatile. Per scoprire come funziona il programma basta leggere il prossimo numero di Hackers Magazine (il 49)!

:: Perché li stanno togliendo

Qualcuno forse ricorderà che, quando esplose il fenomeno degli MP3, Sony (uno dei più acerrimi avversari della pirateria audiovisiva) rilasciò il player OpenClip, che implementava una protezione di basso livello di DRM (Real o OpenMG) che di fatto impediva il libero scambio dei contenuti. In quel periodo tutti conoscevano Kazaa e Napster e tutti si tennero alla larga dall'OpenClip! Il Walkman (inventato proprio da Sony) stava morendo e Sony lanciava un prodotto sostitutivo che il mercato non voleva: un suicidio commerciale!
Lo stesso problema si poneva con la trasformazione di un CD audio in formato WMA (Windows Media Audio), un formato supportato solo sui PC e solo con Windows e legato alla particolare installazione di Windows: formattando e reinstallando il formato non veniva più riconosciuto come legittimo anche se il PC e l'utilizzatore erano gli stessi!
Ma ci sono problemi più gravi: il DRM non è esente da errori. Si tratta pur sempre di un software, non esente quindi da bachi e falle di sicurezza. Ogni tanto anche Microsoft deve aggiornare questa protezione per fronteggiare nuovi problemi che derivano dalla complessità su cui si basa il controllo delle licenze integrato in Windows Media Player.
Esistendo una normativa che impedisce di studiare il DRM, di fare reverse engineering, di creare strumenti o fornire informazioni che ne impediscano il funzionamento, chi impedisce ai suoi grandi promotori di inserire al suo interno meccanismi che con un eufemismo potremmo definire inattesi? Sempre Sony è stata accusata di aver inserito spyware all'interno di SunnComm MediaMax, una tecnologia DRM impiegata su CD musicali che una volta inseriti in un PC installano diversi mega di dati anche se non si accetta la licenza al setup! Questo software comunica con i server della Sony in maniera silente senza alcun preavviso e senza alcuna autorizzazione da parte dell'utente.
E la beffa è che SunnComm, grazie a questo suo opinabile comportamento, apre anche la porta a malintenzionati in grado di sfruttare la falla di sicurezza che ha aperto.
Siamo ben oltre le premesse di tutela e controllo dei diritti d'autore!

Massimiliano Brasile

ITUNES: NO DRM

Da un po' di tempo anche Apple sta proponendo brani senza DRM sul suo iTunes Store. Si tratta dei brani che fanno parte di iTunes Plus: costano 1,29 € a brano, ma sono codificati a 256 Kbps anziché i soliti 128 e non contengono protezione DRM, quindi possono essere ascoltati su qualunque PC o dispositivo.



Cronaca di una guerra che ha colpito una delle principali piaghe del web

MCCOLO: CRONACA DI UNA BATTAGLIA!

Per quanti si fossero sintonizzati sul pianeta Terra solo ora, ecco un brevissimo riassunto dei fatti. Lo scorso Novembre, dopo quattro mesi di duro lavoro, un gruppo composto da esperti di sicurezza con l'aiuto degli autori del blog Security Fix sul sito del Washington Post, ha raccolto prove sufficienti a dimostrare che l'ISP McColo era legato a un vasto network di spam e di diffusione illegale di materiale coperto dal diritto d'autore.

Così, i due provider della connessione all'ISP, Hurricane Electric e Global Crossing, verificata la cosa, hanno deciso di tagliare l'approvvigionamento di banda, sancendo la fine di McColo stesso. Il risultato? Inaccessibilità del sito www.mccolo.com a parte, lo spam a livello mondiale è calato di circa il 66%. Un dato impressionante, che oltre a togliere ogni dubbio su una ben poco credibile coincidenza, dimostra che il fenomeno della "pubblicità indesiderata" non é così frammentato come si crede, ma dipende da pochi, grossi, protagonisti. Dopo pochi giorni, a dircela tutta, lo spam ha ricominciato a circolare più invadente che mai ma la vittoria è stata comunque importante. Vediamo come è stato possibile.



Archive.org ci mostra l'immagine del fu Mccolo.com. Notare, sulla destra, la possibilità di tradurre i testi in russo, e il messaggio che avverte che qui non si tollera lo spam… ah ah ah!

:: In principio fu la botnet

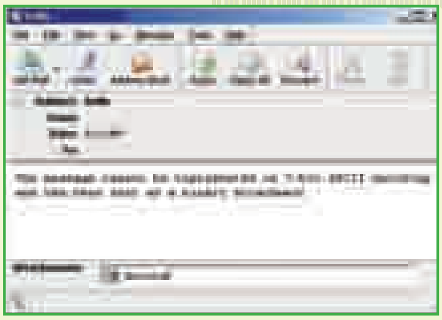
E come possono, queste vere e proprie organizzazioni criminali informatiche, riuscire a diffondere una così impressionante quantità di e-mail? Si appoggiano alle così dette "botnet", cioè reti di computer infettati da trojan. Una volta che i truffatori informatici controllano i computer di una botnet, li usano per diffondere i loro messaggi di posta elettronica o per ampliare la botnet stessa, con l'invio di altri trojan. Va da sé che, per ricercatori e investigatori, non è certo semplice seguire il percorso a ritroso, partendo cioè da alcune e-mail di spam per poi arrivare alla fonte. Tanto che i (circa) quattro mesi di lavoro richiesti per lo smascheramento di McColo hanno il sapore del miracolo digitale.



Alan Ralsky è stato accusato, nel 2008 non solo di spam ma anche di frodi economiche.

:: Una vecchia conoscenza

È pur vero che, per portare a termine l'operazione, ci si è rivolti anche a precedenti fatti di "cronaca informatica", il principale è quello che ha coinvolto lo spammer Alan Ralsky, beccato con le mani nel sacco nei primi mesi del 2008. Ma cos'ha a che fare Ralsky con McColo? Molto, e per capirlo scopriamo come lavorava prima del suo arresto.



Warezov in azione, con una e-mail inviata da una botnet.

:: Da Warezov in poi

In pratica, il truffatore informatico utilizzava il malware Warezov (anche conosciuto come Stration o Opnis) per infettare dei computer e creare, appunto, una botnet. Warezov si propaga di solito come allegato nelle e-mail, ma le contromisure predisposte anche dai più banali antivirus, che bloccano i file eseguibili sospetti, ha obbligato spammer e gestori di botnet a cambiare strategia.
Ecco dunque che Warezov ora si installa come plugin o programma stand-alone, dai siti web, invogliando l'utente al download tramite social engineering. Una volta che il programma è installato, funziona tramite payload, con il truffatore che può operare sul computer infetto come meglio crede. Nel caso di spammer come Ralsky, in particolare, i computer infetti prestano il loro indirizzo IP per diffondere le e-mai pubblicitarie, mascherando l'indirizzo originario.
Per evitare blocchi della botnet, però, è necessario che gli indirizzi IP possano essere cambiati tra loro a gran velocità, ed è per questo che Warezov installa nel computer infetto due componenti: un proxy HTTP che riceve il "contenuto" dal server di partenza, e un server DNS basato su una versione modificata del noto software ISC BIND. Così, il server DNS di ciascun computer infetto è regolarmente aggiornato rispetto al server di partenza, trovandosi "alla pari" con gli altri e permettendo, appunto, un'alta "rotazione" degli indirizzi IP.

:: McColo alla ribalta

Discorso chiuso? Assolutamente no: se molte domande trovano risposta in quanto appena detto, è pur vero che all'appello manca ancora qualcuno. Vale a dire il succitato "server di partenza", o "master server". Warezov in passato era legato ai server di Atrivo/Intercage, ma la loro chiusura (operata con azione simile a quella contro McColo) lo ha obbligato a spostarsi altrove. E, più precisamente, su alcuni server di McColo Corporation, un provider americano. Per evitare grane in patria ha preferito essere inviso agli spammer russi: questi gli hanno così "affidato" la gestione delle principali botnet del mondo, vale a dire Pushdo/Cutwail, Ozdok/Mega-D, Rustock e Srizbi.

:: La battaglia finale

Sulla base di queste considerazioni (ovviamente stiamo semplificando di molto il discorso), i ricercatori hanno osservato per qualche mese il comportamento di Warezov e di queste botnet. In effetti per inchiodare McColo non serviva dimostrare l'entità del traffico illegale che generava: bastava solo qualche e-mail. Per farlo, i ricercatori hanno fatto da "vittime", lasciando infettare alcuni computer e analizzandoli costantemente. Una volta scoperto che buona parte delle infezioni avevano la sintomatologia tipica di Warezov, è stato sufficiente controllare il routing del traffico dati per risalire a McColo. Carte alla mano, il gruppo di ricerca ha reso conto dell'indagine, come detto, a Hurrican Electric e Global Crossing, che hanno confermato i sospetti, bloccando la fornitura di rete a McColo. Gli stessi ricercatori non si aspettavano certo che, a quel punto, lo spamming mondiale calasse dal 60 al 75%, nei giorni successivi alla chiusura, e hanno cantato vittoria. Una vittoria effimera, dato che, meno di un mese dopo, il livello di spam è tornato a crescere già del 37%. Del resto, come in ogni organizzazione criminale che si rispetti, sparito un "boss" se ne fa un altro. E la guerra continua.

Riccardo Meggiato



Un semplice software, qualche accortezza, ed eccoci trasformarti in campioni dei videogiochi

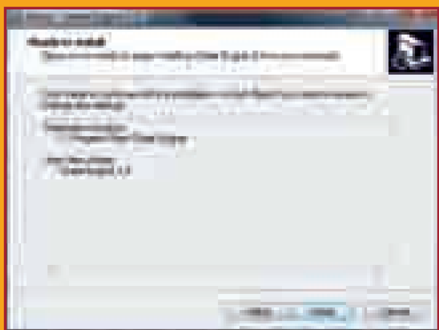
Bariamo con i giochi Flash online

Una premessa doverosa: ciò che stiamo per spiegare ha dell'incredibile. Parliamo, infatti, di un sistema di hacking col quale farci beffe degli avversari nei giochi Flash preferiti. E ora, via con la nostra nuova avventura...

Il futuro dei videogiochi ha sempre più i colori del web. E non parliamo "solo" di titoli con modalità online, ma anche di tutti quelli fruibili direttamente dal nostro browser. Ci sono infatti i "browser game", di solito semplici strategici o manageriali a base di testi e grafica striminzita, ma anche i giochi "flash", che prendono il loro nome dall'utilizzo del software di Adobe. Cos'è, nella sua essenza, Flash? La possiamo definire una "tecnologia", perché offre strumenti sia per godere di grafica e audio di qualità nei siti web, sia per sviluppare contenuti evoluti sfruttando il suo linguaggio ActionScript. Un momento: abbiamo parlato di linguaggio?

::Un linguaggio, per iniziare

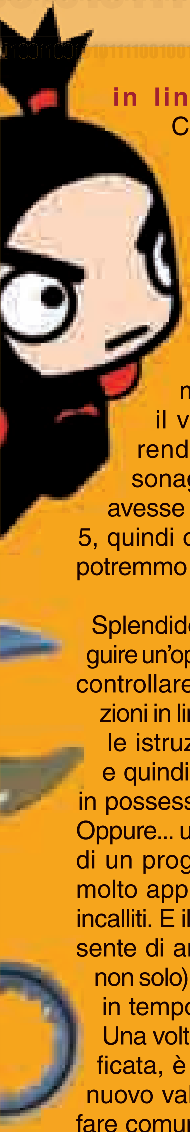
Proprio così: i videogiochi Flash sono prevalentemente realizzati sfruttando questo linguaggio "interno" di Flash stesso. E dato che un videogioco è a tutti gli effetti un programma, è dotato di innumerevoli variabili, che gestiscono sia le sue funzioni di base, sia i parametri che poi vengono visualizzati al videogiocatore di turno. Un esempio? Una variabile, in un gioco d'azione, può essere DIREZIONE. E questa può assumere, sempre rimanendo nel nostro esempio, i valori 0, 1, 2 o 3; a seconda che la direzione sia avanti, indietro, sinistra o destra. Similmente, ci può essere anche una variabile che si chiama ENERGIA, che tiene conto della quantità di energia rimasta al giocatore. Per esempio, con un valore tra 0 e 100. Ovviamente, quando l'energia arriva a zero il giocatore muore. Caput.



Bastano pochi clic per installare Cheat Engine nel nostro computer.

::Verso l'esadecimale

Un programma ActionScript, con tutte le sue variabili, per essere compreso dal computer è trasformato



in linguaggio esadecimale. Così, per esempio, le variabili DIREZIONE ed ENERGIA, con i rispettivi valori, sono convertite in questo linguaggio piuttosto ostico da capire per una mente umana. E perché mai, in fondo, lo si dovrebbe capire? Perché se, per esempio, fosse possibile modificare, in tempo reale, il valore ENERGIA, potremmo rendere immortale il nostro personaggio! Per esempio, se questi avesse un valore di ENERGIA pari a 5, quindi ormai prossimo alla morte, lo potremmo riportare a 100!

Splendido, vero? Peccato che per eseguire un'operazione del genere dovremmo controllare lunghissimi elenchi di istruzioni in linguaggio esadecimale (perché le istruzioni originali, in ActionScript e quindi a noi più comprensibili, sono in possesso solo dell'autore originario!). Oppure... utilizzare Cheat Engine! Si tratta di un programma, totalmente gratuito, molto apprezzato dai game-hacker più incalliti. E il motivo è molto semplice: consente di analizzare un gioco Flash (ma non solo) in esecuzione, e di modificarne in tempo reale il valore delle variabili! Una volta che la variabile è stata modificata, è utilizzata dal programma col nuovo valore. In realtà abbiamo a che fare comunque col codice esadecimale, ma in modo così semplice che quasi non ce ne accorgeremo.

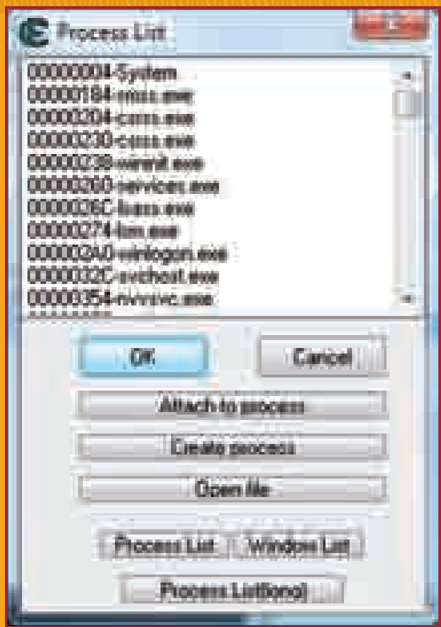
::Si parte dall'installazione

Il primo passo sta nell'installare ovviamente Cheat Engine. Per farlo, andiamo su www.heijnen1.demon.nl/#DCET, e scarichiamo la versione più recente. Al momento è la 5.4, che troviamo direttamente su www.heijnen1.demon.nl/CheatEngine54.exe. Scaricato il file, facciamoci sopra doppio clic e avviamo la procedura d'installazione. Clicchiamo su Next, spuntiamo I accept the agreement, clicchiamo ancora su Next, fino alla fine.

Nell'ultima finestra, clicchiamo su Install. Al termine, clicchiamo su Next. Se utilizziamo Windows Vista, togliamo il segno di spunta dalla casella, poi clicchiamo su Finish. Vista ha bisogno di avviare il programma con tutti i privilegi di sistema: per farlo, selezioniamo Start/Tutti i programmi/Cheat Engine 5.4, clicchiamo col tasto destro del mouse su Cheat Engine 5.4, selezioniamo Esegui come amministratore, poi clicchiamo su Consenti. Clicchiamo su Yes e poi su No.

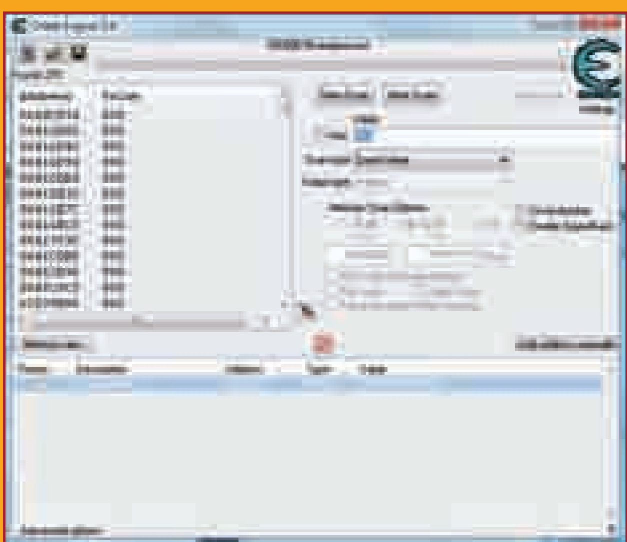
Una volta installato il programma, vediamo di chiudere TUTTE le finestre di Internet Explorer aperte, e lasciare attiva solo quella dove andiamo a caricare il nostro gioco (o dove è già stato caricato). Tra l'altro, non ci devono essere schede multi aperte. Fatto questo, avviamo pure il titolo. Mettiamo che si tratti di uno sparatutto, dove la voce Points riporta il nostro punteggio, pari ora a 100. Andiamo in Cheat Engine, clicchiamo sull'icona in alto a sinistra (a forma di computer), scorriamo la Process List fino a trovare iexplore.exe.

Clicchiamoci sopra e poi clicchiamo su Ok. Tornati alla finestra iniziale di Cheat Engine, in Value scriviamo il valore del punteggio e, selezionando in Value Type la voce Double, clicchiamo su First Scan. A sinistra compare una serie di indirizzi di memoria. Torniamo al gioco, proviamolo ancora di modo da aumentare il punteggio, poi passiamo di nuovo a Cheat Engine.



Con una sola finestra (e scheda) attiva di Explorer, non rischiamo di sbagliare la selezione del "processo".

Scriviamo il nuovo valore del punteggio in Value, e questa volta clicchiamo su Next Scan. Così restringiamo la ricerca agli indirizzi di memoria nei quali è stato variato il precedente valore 100, nel nuovo valore. Se ne resta uno (in caso contrario ripetiamo l'operazione con un nuovo punteggio), facciamoci sopra doppio clic. Viene così spostato in basso. Facciamo doppio clic sul valore che troviamo nella colonna Value (e che è pari al nuovo punteggio), quindi cambiamolo, col punteggio che desideriamo. Clicchiamo su OK. Il valore della variabile è stato cambiato, e per vederlo "in azione", sarà probabilmente necessario giocare un po' col titolo e attendere che il punteggia venga variato, mostrando poi quello "ritoccato". Questa procedura funziona spesso, ma non sempre. Tra le possibili cause di malfunzionamento, c'è l'utilizzo di Flash diverso e superiore dalla versione 7 (quindi 8 o 9). In questo caso, quando effettuiamo la ricerca del valore, scriviamolo in Value moltiplicato per 8. Se è 100, per esempio, scriviamo 800. In Value type, invece, selezioniamo 4 Bytes.



Se utilizziamo Flash 8 o 9 dobbiamo seguire una procedura leggermente diversa.

GPS hacking & unlock

Libera il tuo navigatore satellitare

Premettiamo che ogni attività di modifica hardware o software su un dispositivo elettronico condotta senza il supporto tecnico o comunque al di fuori dei locali autorizzati ad effettuare tale modifica di fatto fa decadere la garanzia. Andiamo comunque a vedere cosa si può fare se non ci preoccupiamo troppo di compromettere il funzionamento del nostro giocattolo dotato di GPS. In ogni caso è buona norma fare un backup completo che ci permetta di ripristinare la situazione iniziale nel caso qualcosa andasse storto o semplicemente non fossimo soddisfatti delle modifiche fatte.

I dispositivi venduti come navigatori satellitari sono effettivamente dei mini-PC, dotati di sistema operativo, monitor LCD (a volte anche touch-screen), porte di comunicazione (USB, infrarossi), qualche giga di flash e diversi mega di RAM. Ma questa ricca dotazione hardware sembra davvero sprecata se pensiamo alla frequenza di clock dei processori che vengono integrati e alla dotazione di memoria a disposizione. Infatti al di là dei normali aggiornamenti software, previsti dal contratto e dalla licenza del produttore, non è possibile ufficialmente modificare il funzionamento principale per il quale viene venduto, ossia fare il navigatore. Ma se andiamo più a fondo e guardiamo cosa c'è sotto quell'interfaccia carina scopriamo che possiamo ottenere molto di più.

:: Perché si può fare

In generale questi dispositivi sono pensati per un utilizzo stand-alone abbastanza limitato: lo accendi, imposti la rotta, arrivi a destinazione, lo spegni. In modelli più costosi vengono aggiunte piccole applicazioni, ma comunque non si pensa a problemi come quello della sicurezza, dal momento che dif-



ficilmente andranno "in rete" e se riceveranno degli aggiornamenti si tratterà solo di quelli relativi al software di navigazione, magari trasmessi tramite il software proprietario del produttore. Né vengono venduti come periferiche general-purpose così come avviene per un personal computer. Addirittura la memoria interna può essere appena sufficiente a contenere le mappe e gli aggiornamenti vanno obbligatoriamente installati su quella esterna.
Ma molti navigatori montano una versione di Windows CE o Windows Mobile. Quindi già sappiamo che il processore del navigatore sarà basato sulla famiglia Intel, o Arm, o Mips ampiamente diffuse. E come ogni ambiente Windows che si rispetti la sicurezza non è il massimo! È infatti possibile modificare lo splash screen o settaggi nascosti, o anche aggiungere programmi già compilati in grado di funzionare senza ulteriori configurazioni. Inoltre è divertente personalizzare il proprio dispositivo anche solo per renderlo diverso da tutti gli altri!

:: Cosa si può fare

La libertà di poter sfruttare al meglio il proprio dispositivo dipende principalmente dalla possibilità o meno di poter accedere direttamente al file system e lanciare programmi caricati su una memoria esterna, come la SD card.
Data la vastità dei prodotti ormai in commercio, non è possibile fornire una guida unica al modding dei navigatori, ma è possibile identificare una serie di modifiche che possono accomunare famiglie di dispositivi di diversi produttori.



Di seguito alcuni degli esempi che variano per tipologia e complessità.

:: Magellan 3100

Il Magellan 3100 è gestito da Windows CE e su questo dispositivo è possibile modificare molto semplicemente lo splash-screen con uno di proprio gradimento.
Basta collegarlo con il cavo usb e modificare (o sovrascrivere) l'immagine presente all'indirizzo F:\APP\TNShell_Bitmap\Venus2\SplashScreen_V2_Animation1.bmp (avendo l'accortezza di salvare in formato bmp e risoluzione 320x240) dopodiché scollegando il cavo si otterrà un soft-reset che ci permetterà di vedere la prima modifica già realizzata.
È poi possibile spostare le mappe su una memoria SD, invece di lasciarle nella limitata memoria interna. Vanno copiati su \MAP\ della SDCARD i quattro file:

- Index.mct
- NRBM_NA.MGI
- US48.IMI
- US48_POI.POI

e poi, dopo aver fatto un backup, va modificato il file di configurazione F:\APP\Media.cfg (Figura 1).
In questo modo (al successivo avvio) i dati verranno caricati dalla SD.

[Figura 1]

```
# Basemap
\SDMMC Card\MAP

# Detailmap Map Data
\SDMMC Card\MAP

# POI Map Data
\SDMMC Card\MAP

# User Data
\HDD\USR

# Sound files data
\HDD\APP

# SD Card simulation directory
\SDMMC Card
```

È possibile poi installare un file manager usando un vecchissimo trucco in piedi dai tempi del DOS! Al boot del dispositivo viene infatti lanciato l'eseguibile F:\APP\Navigator.exe. È sufficiente quindi rinominarlo (ad esempio in GPSNavigator.exe), per poter sostituire tranquillamente il manager da lanciare all'avvio (es. la versione per ARM del Windows CE File Manager disponibile a questo link http://bbs.100gps.com/attachment.php?aid=14343). Una volta scaricato il file, va decompresso e tutti i file che iniziano con FM_ e il file FileManCE.exe vanno copiati in F:\APP; chiaramente FileManCE.exe andrà rinominato in Navigator.exe.
A questo punto scollegando il cavo si otterrà un soft-reset e partirà il file manager. Per avviare l'applicazione andrà selezionato e lanciato il file F:\APP\GPSNavigator.exe.

:: TomTom GO

Sperimentata dall'autore sul TomTom ONE V3, è stata rilasciata una console in stile bash per la famiglia TomTom GO (www.opentom.org).
Tramite la tastiera virtuale (e pennino) è possibile inserire direttamente i comandi da eseguire e si possono lanciare altri programmi, precedentemente caricati sulla SD, come il player MP3 Madplay o lanciare il porting dell'ambiente di sviluppo x11-basic che permette di realizzare in basic le proprie applicazioni grafiche.
La TTConsole implementa un'emulazione di terminale a colori con un piccolo font che sfrutta il frame-buffer e supporta le interfacce touchscreen.
È possibile poi aggiungere una versione apposita di pico in modo da avere anche un editor testuale.
Ovviamente si può lanciare un player



MP3 come Madplay e un video player come MPlayer che non ha bisogno di presentazioni e che supporta un ampio ventaglio di formati.

:: MioPocket 2.0

MioPocket differisce dalle altre soluzioni perché rappresenta un vero kit di tuning. È un concentrato di software, script, file di registro, skin realizzato per i navigatori GPS della serie Mio basati su PocketPC (PDA), che fornisce in un'unica soluzione un media player (audio e video), tre lettori di e-book (che includono due dizionari), svariati giochi, due viewer per immagini, due programmi di disegno, visualizzatori di documenti MS Office, editor testuali, un manager per le rotte di MioMap, quattro applicazioni che visualizzano il GPS, un'applicazione per appuntamenti, una calcolatrice, un convertitore di unità, editor di registro, task manager, file manager, una sveglia e altre applicazioni.



Il player supporta molti formati video, ma il bitrate deve essere compreso tra 500-1000Kb/s per avere sufficiente fluidità. I dispositivi supportati sono marchiati Mio, ma è possibile che funzioni anche su altri dispositivi. In particolare:

- **c320 e c520**: completamente supportati
- **c620, c720, c310x, c510 e c710**: quasi tutto dovrebbe funzionare
- **c220, c230 e tutti i modelli Moov**: la maggior parte delle cose dovrebbe funzionare; è possibile che ci siano alcuni problemi non critici
- **c250, 268+, h610 e alcuni dispositivi non marchiati Mio (come Magellan Maestro, Navigon, Harman Kardon e Asus)**: si sa che funziona, ma ci si aspetta che ci siano dei piccoli problemi

È possibile scaricare il kit all'indirizzo http://www.gpspassion.com/forumsen/topic.asp?TOPIC_ID=109690 e, dopo averlo decompresso sul PC (non decomprimerlo direttamente sulla SD!) si può passare all'installazione sul navigatore (consigliamo di installarlo sulla SD in modo da evitare modifiche accidentali al file system e poter tornare facilmente indietro). Una guida dettagliata è disponibile all'indirizzo http://www.gpspassion.com/upload2/MioPocket%20Readme.html.
Per la maggior parte dei Mio, la procedura consiste nel copiare e rinominare MioAutoRun.exe sulla SD in accordo al modello di navigatore che si possiede (es. MioAutoRun.exe →c310Auto.exe sul modello c310). Dopodiché va inserita la SD nel dispositivo e una finestra notificherà l'avvenuta installazione del kit!
MioPocket supporta anche le schede SDIO WiFi che trasformano il navigatore GPS anche in un terminale di una rete WLAN. Le schede supportate sono la Ambeon WL54C-SD e le due Spectec SDW-820 e SDW-821.



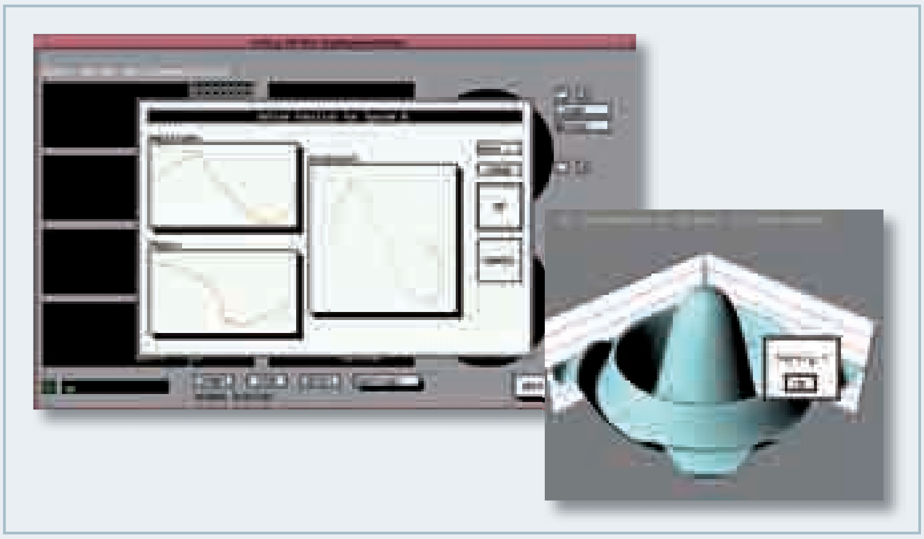
Alcune tra le varie interfacce alternative che si possono usare su MioPocket 2.0.

:: Il percorso inverso: aggiungere il GPS alla PSP

In questo caso dobbiamo armarci di un saldatore, multimetro e un po' di materiale, oltre ad avere una PSP con firmware di versione superiore alla 2:

- l'antenna GPS (Holux GPSlim236, circa 60 €)
- cavo di controllo remoto della PSP Intec G6704 (circa 15 €)
- un cavo USB Mini B (circa 5 €)
- una resistenza 1 Kohm 1/4 watt (circa 1 €)
- nastro isolante (circa 2 €)

Si tagliano il cavo USB (dal quale si recupera il connettore Mini B) e il G6704 e si realizza un nuovo connettore adatto alla PSP che sfrutta il connettore Mini B e il jack per l'alimentazione dell'antenna. Tra il pin GPS TXD (pin 3 Mini B) e il pin PSP RX (pin 2 G6704) va posizionata la resistenza in modo da ottenere una tensione compresa tra 3.2V e 5V (potrebbero quindi servire altre resistenze per trovare il valore ottimale), mentre va connesso direttamente il pin GPS GND (pin 1 Mini B) al pin PSP GND (pin 2 G6704).
Una volta che il multimetro ci conferma le connessioni e la tensione che arriva, fissiamo il nuovo connettore con del nastro isolante, lo inseriamo nella PSP e installiamo il software gratuito GPS Viewer (http://deniska.dcemu.co.uk/bin/gps_viewer.zip). Se abbiamo il segnale GPS, vedremo comparire le coordinate sulla nostra console.



Alcune schermate di x11-basic in funzione su un PC Linux.

:: Cosa occorre (sw/hw)

In generale per poter aggiungere nuove funzionalità a questi dispositivi, è sufficiente agire tramite SD card, quindi l'ideale è disporre di un lettore di memorie del tipo usato dal nostro dispositivo. Se lo abbiamo siamo già a buon punto perché possiamo creare file system da zero, fare backup sul PC e copiare file da testare. Ormai se ne trovano anche a pochi euro, soprattutto se non ci interessano i modelli all-in-one, ma quelli in grado di leggere il solo formato che ci occorre. Da Windows XP in poi o con Linux non occorre neanche un driver, dal momento che il lettore diventa un'estensione del protocollo USB e la memoria viene vista come un'unità rimovibile (come accade per le pendrive USB).
Nel caso non si disponga di questo specifico lettore, è di solito possibile usare lo stesso dispositivo in modalità lettura/scrittura, chiaramente a velocità più ridotte e a volte con funzionamento più limitato.



Le modifiche hardware da apportare al cavo della PSP per usarla come GPS.

:: Conclusioni

Il bello di andare sotto la superficie delle cose è quello di riuscire a vedere a volte delle caratteristiche che per ragioni di marketing o semplicemente di utilità vengono nascoste all'utente. Con l'introduzione sul mercato di dispositivi evoluti, quali sono i navigatori e le console per videogiochi, ci ritroviamo tra le mani dei concentrati di tecnologia che sono in grado letteralmente di trasformarsi con piccole modifiche.

E oltre al divertimento di riuscire ad avere un player MP3 o un video player in un dispositivo che sembrava utile solo qualche volta in auto, possiamo capire meglio come funziona, così se un domani il navigatore non dovesse più avviarsi saremo in grado di ripristinarlo senza ricorrere all'assistenza tecnica.

Massimiliano Brasile